

Klaus-Rainer Müller

IT-Sicherheit mit System

Leserstimmen zu vorangegangenen Auflagen:

„Sehr klar und ansprechend. Das beste Grundlagenbuch für den Management-Ansatz!“

Prof. Dr. H. M. Winkels, FH Dortmund

„/.../ empfehle ich meinen Studenten, weil es eines der wenigen Bücher zur Sicherheit ist, das gut strukturiert ist.“

Prof. Dr.-Ing. Damian Weber, HTW Saarbrücken

„Das Buch ‚IT-Sicherheit mit System‘ trifft genau meinen Geschmack. Es ist sachlich und verzichtet auf unnötige Angstmacherei, ohne dabei Sicherheitslücken zu beschönigen. Sehr strukturiert, methodisch und auf dem notwendigen Abstraktionslevel wird auf die Bedürfnisse der Zielgruppe /.../ eingegangen. /.../ Der Autor hat offensichtlich genug Praxiserfahrung, um zu sehen, worauf es ankommt.“

amazon.de, 07/2004

Pressestimmen zu vorangegangenen Auflagen:

„‘IT-Sicherheit mit System‘ wird durch die konsequent strukturierte Vorgehensweise seinem Titel durchaus gerecht [...] und bietet dem Leser ein sehr praxisorientiertes Werkzeug, um das Sicherheitssystem seines Unternehmens aufzubauen oder kritisch zu prüfen.“

Wirtschaftsinformatik, 06/2006

„[Dem Buch] merkt man sofort an, dass es von einem waschechten Experten geschrieben wurde. Das Themenspektrum ist so durchdacht, dass man am Ende nicht mehr glauben will, dass es jemals ohne dieses Prinzip geklappt hat. [...] Es sind im Vergleich zur ersten Aufgabe nicht weniger als 14 Themen hinzugekommen.“

hakin9, 02/2007

Klaus-Rainer Müller

IT-Sicherheit mit System

**Sicherheitspyramide – Sicherheits-,
Kontinuitäts- und Risikomanagement –
Normen und Practices – SOA und
Softwareentwicklung**

3., erweiterte und aktualisierte Auflage

Mit 36 Abbildungen



Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <<http://dnb.d-nb.de>> abrufbar.

Das in diesem Werk enthaltene Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials oder Teilen davon entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne von Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2003
2. Auflage 2005
- 3., erweiterte und aktualisierte Auflage 2008

Alle Rechte vorbehalten

© Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden 2008

Lektorat: Sybille Thelen / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.

www.vieweg.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de

Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Printed in Germany

ISBN 978-3-8348-0368-9

Vorwort

Welches Ziel verfolgt dieses Buch?

Effiziente Existenz- und Zukunftssicherung des Unternehmens sowie zielgerichtete Risikosteuerung sind entscheidende Managementaufgaben. Ihre Bedeutung wächst rasant aufgrund gesetzlicher Vorgaben wie KonTraG und Regularien wie Basel II, Solvency II und MaRisk. Wirtschaftliches, transparentes und durchgängiges Sicherheits-, Kontinuitäts- und Risikomanagement sind gefordert. Daher sind Investitionen notwendig, deren Umfang von der Effizienz und Effektivität des Sicherheitsmanagements abhängt.

Die Problemstellung

Trotz dieser hohen Bedeutung und der Haftungsrisiken weist die Sicherheits- und Risikosituation in Unternehmen häufig Defizite auf, z. B. hinsichtlich Zielen, Strategie, Struktur, Transparenz sowie anforderungsgerechter Umsetzung und Effizienz. Hinzu kommt eine Fokussierung des Sicherheits-, Kontinuitäts- und Risikomanagements auf den IT-Betrieb. Dadurch erfolgt oftmals keine oder eine nur unzureichende Integration in die IT-Prozesse sowie den Lebenszyklus von IT-Prozessen und -Systemen.

Vor diesem Hintergrund habe ich die dreidimensionale Sicherheitspyramide entwickelt. Sie ist top-down strukturiert und berücksichtigt die IT-Prozesse, die IT-Ressourcen sowie den IT-Lebenszyklus. Sie dient als systematisches und ingenieurmäßiges Vorgehensmodell für den Aufbau und die Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements. In ihren mehrdimensionalen Rahmen können Sie die unterschiedlichsten Sicherheits-, Kontinuitäts- und Risikothematiken „einklinken“. So lassen sich Defizite reduzieren oder beseitigen und die Effizienz durch Standardisierung steigern.

Die Lösung

Die Sicherheitspyramide nach Dr.-Ing. Müller stellt ein gesamtheitliches, systematisches und dadurch effizientes Vorgehensmodell dar. Sie integriert auf innovative Weise neben den Disziplinen Sicherheits-, Kontinuitäts- und Risiko- sowie Compliancemanagement Kernelemente und -methodiken, die in der folgenden Aufzählung angegeben sind. Diese kommen, wenn auch in unterschiedlicher Ausprägung, Vollständigkeit, Detaillierung, Konkretisierung und Qualität sowie teilweise nach Erscheinen meiner Publikationen in bestehenden Standards und Practices vor:

Alleinstellungsmerkmal der Sicherheitspyramide

- der PDCA-orientierte Sicherheits- und Kontinuitätsprozess
(die ISO 27001:2005 nutzt ebenfalls einen PDCA-orientierten Sicherheitsprozess,
die BS 25999-1:2006 fordert in der BCM-Politik Prozesse zum Aufbau, zur Steuerung und Pflege des BCM, also einen Kontinuitätsprozess)
- die Sicherheitshierarchie
(die ISO 13335-1:2004 und die BSI-IT-Grundsatzkataloge seit 2005 enthalten Teilbereiche einer Sicherheitshierarchie)
- die Sicherheits-, Kontinuitäts- und Risikopolitik
(die ISO 27001:2005 fordert eine Informationssicherheitsmanagementpolitik {ISMS-Politik},
die BS 25999-1:2006 eine Kontinuitätspolitik)
- die IT-Prozesse und deren Sicherheitsanforderungen
(ITIL® und die ISO 20000-1:2005 beschreiben Teile jener IT-Prozesse, die in der Sicherheitspyramide enthalten sind)
- der Lebenszyklus von IT-Prozessen, IT-Ressourcen einschließlich IT-Systemen, IT-Produkten und IT-Leistungen (Services)
(die ITSEC/CC enthalten ein Lebenszyklusmodell für IT-Produkte und -Systeme,
die ISO 13335-1 spricht im Jahr 2004 überblicksartig erstmals das Thema Lebenszyklus-Management an,
in den BSI-IT-Grundsatzkatalogen findet sich seit Ende 2006 in Form der Maßnahme M 2.378, System-Entwicklung, eine überblicksartige Beschreibung des Lebenszyklus für IT-Systeme,
ITIL®, Version 3, führt im Jahr 2007 einen IT-Service-Lebenszyklus {Lebenszyklus Leistungen/Dienste} ein,
COBIT® streift den Lebenszyklus im Rahmen des Projekt- und Qualitätsmanagements)
- der Sicherheitsregelkreis
(COBIT® benennt eine Vielzahl von Kontrollen für diverse Prozesse/Managementdisziplinen der IT,
die Balanced Scorecard beschreibt ein allgemeines mehrdimensionales Steuerungssystem mit Leistungskennzahlen {KPI})
- das integrative Sicherheits-, Kontinuitäts- und Risiko- sowie Compliancemanagement
(die ISO 27001:2005 betrachtet das Sicherheits- und Risikomanagement und enthält Kontrollen zum Sicherheitsmanagement, zu BCM und zu Compliance)

- die Berücksichtigung der gesetzlichen, aufsichtsbehördlichen, normativen und vertraglichen Konformität (compliance)
(die ISO 17799:2005, die seit Juli 2007 ISO 27002:2005 heißt, geht auf compliance ein, die ISO 27001:2005 nennt Kontrollen hierzu)
- die Sicherheitsrichtlinien, -konzepte und -maßnahmen
(die IT-Grundschutzkataloge des BSI und die ISO 17799:2005 bzw. ISO 27002:2005 widmen sich diesen in unterschiedlicher Ausprägung, Detaillierung und Konkretisierung)

Die 1995 erstmals vorgestellte Sicherheitspyramide [1] lässt sich für die gesamte Palette von Sicherheitsthemen eines Unternehmens nutzen. Dieses Buch beschreibt sie in der Version IV unter dem Fokus der IT- bzw. ITK-Sicherheit (IT + TK = ITK). Dementsprechend heißt sie IT- bzw. ITK-Sicherheits- bzw. -Sicherheitsmanagementpyramide, kurz ISiPyr, ITK-SiPyr (ISP), ISimPyr oder ISMP. Sie berücksichtigt das Sicherheits-, Kontinuitäts- und Risiko- sowie Compliancemanagement.

*Die Reichweite
der Lösung*

Das Buch bietet Ihnen durch die Struktur der Sicherheitspyramide das notwendige Handlungswissen, um die ITK, ihre Prozesse, Ressourcen und Organisation sowie den ITK-Lebenszyklus systematisch, anschaulich, effizient und ganzheitlich auf ITK-Sicherheit auszurichten. Neben den Erläuterungen illustrieren Abbildungen die Sachverhalte. Checklisten, Gliederungen und Tabellen aus der Beratungspraxis beschleunigen den Einstieg.

*Das
Handlungs-
wissen*

Wer sollte dieses Buch lesen?

Der Titel sagt es bereits – das Buch richtet sich an Leserinnen und Leser, die sich direkt oder indirekt mit der IT-Sicherheit befassen:

- IT-Sicherheitsbeauftragte, die für die Sicherheit der Informationsverarbeitung insgesamt oder für Teile verantwortlich sind, sollten wissen, wie das Sicherheitsmanagement strukturiert aufgebaut und weiterentwickelt werden kann.
- Chief Information Security Officers, die für die Sicherheit der Informations- und Telekommunikationstechnologie (ITK) im Unternehmen sowie für deren zielgerichteten strategischen Aufbau verantwortlich sind, sollten wissen, wie sich der Schutzbedarf und die Bedrohungslage entwickeln und das Sicherheitsmanagement strategisch und effizient aufgebaut und gesteuert werden kann.
- Chief Information Officers, die für die Informations- und Telekommunikationstechnologie (ITK) sowie für deren Sicherheit verantwortlich sind, sollten wissen, mit welchem Vorgehensmodell

*IT-Sicherheits-
beauftragte*

*Chief
Information
Security
Officers*

*Chief
Information
Officers*

das Sicherheitsmanagement aufgebaut, gesteuert und weiterentwickelt werden kann.

Notfallmanager

- Notfallmanager, die für die Notfall- und Katastrophenvorsorge des Unternehmens insgesamt oder für Teile davon verantwortlich sind, sollten wissen, wie die Notfallplanung zielgerichtet aufgebaut und weiterentwickelt werden kann.

*Sicherheits-
auditoren*

- Sicherheitsauditoren, welche die ITK-Sicherheit im Unternehmen prüfen und weiterentwickeln, sollten wissen, wie diese Prüfungen in das Sicherheitsmanagement eingebettet sind und wie sie durchgeführt werden können.

Risikomanager

- Risikomanager, die für das Risikomanagement im Unternehmen verantwortlich sind, sollten wissen, wie dieses mit dem Sicherheitsmanagement zusammenspielt.

Bereichsleiter

- Bereichsleiter, welche die Informationsverarbeitung zur Unterstützung ihrer Geschäftsprozesse nutzen, sollten wissen, wie sie ihre Anforderungen erheben und an den IT-Bereich weitergeben können.

*Vorstände und
Geschäftsführer*

- Vorstände und Geschäftsführer, die für die Informationsverarbeitung im Unternehmen verantwortlich sind oder sie nutzen, sollten die Entwicklung der Bedrohungslage, die gesetzlichen Rahmenbedingungen und persönlichen Haftungsrisiken kennen und wissen, wie das Sicherheitsmanagement durch eine Sicherheitspolitik und den Sicherheitsregelkreis zielgerichtet und effizienzorientiert gesteuert werden kann.

Wie können Sie dieses Buch nutzen?

*Fragen,
die das Buch
beantwortet*

Das vorliegende Buch beantwortet Ihnen die folgenden Fragen "Wie kann ich ..."

- ... mir einen Überblick über Trends bei Bedrohungen und Schutzbedarf sowie häufige Schwachstellen verschaffen?
- ... das Sicherheitsmanagement zielorientiert und systematisch aufbauen?
- ... mir einen schnellen Überblick über das Sicherheitsmanagement anhand der Sicherheitspyramide verschaffen?
- ... eine Sicherheits-, Kontinuitäts- und Risikopolitik aufbauen?
- ... Sicherheitsziele bzw. Sicherheitsanforderungen ermitteln?
- ... Sicherheitsziele auf die Schutzobjekte, z. B. ITK, abbilden?
- ... eine umfassende Sicherheitsarchitektur konzipieren?
- ... Sicherheitsrichtlinien aufstellen?

- ... Sicherheitskonzepte entwickeln?
- ... die Themen Prozesse, Ressourcen und Organisation in das Sicherheitsmanagement integrieren?
- ... die Sicherheitsschalen transparent gestalten?
- ... das Berechtigungsmodell anschaulich darstellen?
- ... den Lebenszyklus von Prozessen, Ressourcen, wie z. B. Systemen, und Produkten sowie Leistungen berücksichtigen?
- ... Sicherheitsprüfungen durchführen?
- ... den Status des Sicherheitsmanagements verfolgen und steuern?
- ... den Sicherheits(management)prozess konzipieren?

Sie können das Buch darüber hinaus als Nachschlagewerk verwenden, indem Sie die bereitgestellten Checklisten, das Glossar und Abkürzungsverzeichnis, das Verzeichnis über Gesetze, Vorschriften, Standards, Normen sowie das Sachwortverzeichnis nutzen. Kapitel 2 bietet Eiligen einen ersten schnellen Überblick. Sie können das Buch insgesamt oder nur ausgewählte Kapitel lesen. Die Einleitungen der Kapitel geben Ihnen einen Überblick über die jeweils behandelten Themen. Die Zusammenfassungen am Kapitelende sind für den „Schnelldurchlauf“ gedacht.

Außerdem können Sie sich anhand der illustrierenden Abbildungen die Sachverhalte vor Augen führen oder die Checklisten, Gliederungen und Tabellen nutzen, um den Einstieg in die Sicherheitsthematik zu beschleunigen.

Für welche Unternehmensgröße eignet sich der Buchinhalt?

Die vorangegangenen Ausführungen deuten bereits an, dass die hier vorgestellte Vorgehensmethodik einem ganzheitlichen Ansatz folgt. Dies erweckt leicht den Eindruck, dass sie nur für mittlere und große Unternehmen geeignet ist. Ist dies tatsächlich so?

Ich denke: nein. Gesetze, Verordnungen, Standards und Normen gelten meist für alle Unternehmensgrößen. Der Unterschied zwischen großen und kleinen Unternehmen liegt häufig darin, dass sich Umfang, Detaillierungsgrad, Sicherheits- und Regelungsbedarf unterscheiden. Während Sie bei größeren Unternehmen unterschiedliche Standorte, mehrere Gebäude, differenzierte Verantwortlichkeiten, vielfältige und zum Teil komplexe IT-Infrastruktur sowie eigene Softwareentwicklung finden, nehmen die Komplexität und die Sicherheitsanforderungen bei kleineren Unternehmen oftmals ab, sind aber vorhanden. Jedes Unternehmen sollte sich daher Gedanken über Sicherheitsbedarf und Risikofreudigkeit machen.

*Checklisten,
Verzeichnisse,
das Kapitel für
Eilige und
Zusammen-
fassungen
verschaffen
schnell
gezielten
Nutzen*

*Sicherheits-
management:
nur für Groß-
unternehmen?*

*Sicherheits-
management
für jede
Unternehmens-
größe*

*Kleine und
mittlere
Unternehmen
(KMUs)*

Ein häufig auch für kleine und mittlere Unternehmen (KMUs) erforderlicher zusätzlicher Regelungs- und Schutzbedarf wird so manches Mal übersehen und führt dann zu unliebsamen Folgen. Zwar ist es für viele Unternehmen selbstverständlich, dass der Zutritt zu den Räumlichkeiten geschützt ist, dass das Verhalten in Notfällen dokumentiert ist, dass Lizenzen eingehalten werden und dass Vereinbarungen zur Geheimhaltung, zum Datenschutz und zum Surfen im Internet existieren. Auch Datensicherungen und Virens Scanner gehören quasi zum Standard, ebenso wie Firewalls und Spam-Filter.

*Kennen Sie Ihre
Risiken?*

Doch ist bekannt, welche Folgen der Ausfall eines Geschäftsprozesses, der Räumlichkeiten, der IT, der Telefonanlage oder eines Service-Gebers hat und in welcher Kosten-Nutzen-Relation entsprechende Sicherheitsmaßnahmen stehen? Was dürfen Ihre Mitarbeiter? Kennen die Verantwortlichen die gesetzlichen Anforderungen? Werden Datensicherungen an einen sicheren Ort ausgelagert und ihre Lesbarkeit geprüft? Werden Virens Scanner aktuell gehalten?

*Betreiben Sie
eine
angemessene
Unternehmens-
sicherung?*

Zugegebenermaßen: Fragen über Fragen und noch längst nicht alle. Doch ihre Beantwortung liefert einen Beitrag zur Risikolage und durch entsprechende oftmals einfache Umsetzung in der Folge zur Unternehmens- und Existenzsicherung. Geringere Komplexität und Anforderungsfülle bei kleinen Unternehmen führen so zu einem schlankeren Sicherheits-, Kontinuitäts- und Risikomanagement, das aber nichtsdestotrotz ganzheitlich, systematisch und unternehmensbezogen vollständig sein sollte.

Wie ist dieses Buch aufgebaut?

Kapitel 1:
*Ausgangs-
situation und
Zielsetzung*

Das Kapitel 1, Ausgangssituation und Zielsetzung, geht ein auf Entwicklungstrends bei Bedrohungen und Schutzbedarf sowie die Sicherheitssituation in Unternehmen. Ferner erläutert es die Notwendigkeit für ein systematisches und strategisches Sicherheits-, Kontinuitäts- und Risikomanagement.

Kapitel 2:
Überblick

Für Eilige gibt Kapitel 2 einen kurzgefassten Überblick über die Inhalte der Sicherheitspyramide.

Kapitel 3:
10 Schritte

Kapitel 3 nennt Ihnen kurz und prägnant 10 Schritte zum Sicherheits-, Kontinuitäts- und Risikomanagement.

Kapitel 4:
Definitionen

Kapitel 4 stellt verschiedene Begriffe und Definitionen aus dem Sicherheits-, Kontinuitäts- und Risikomanagement vor, die in diesem Buch verwendet werden. Es behandelt u. a. das Sicherheitsmanagement einschließlich Standards und Practices, die ingenieurmäßige Sicherheit, die Sicherheitspyramide und –politik, Ressourcen, Schutzobjekte und –subjekte sowie Sicherheitskriterien, die Business Impact

Analysis, Geschäftskontinuität (Business Continuity), Risikodreiklang und Risikomanagement.

Kapitel 5 gibt eine zusammenfassende Beschreibung des Aufbaus und der Inhalte der dreidimensionalen Sicherheitspyramide des Autors.

*Kapitel 5:
Sicherheits-
pyramide*

Die Kapitel 6 bis 14 beschreiben die einzelnen Elemente der Sicherheitspyramide. Kapitelweise behandelt das Buch zuerst die hierarchischen Ebenen der Sicherheitspyramide, beginnend bei der Sicherheits-, Kontinuitäts- und Risikopolitik, über die Sicherheitsziele, deren Transformation, die Sicherheitsarchitektur, -richtlinien, -konzepte und -maßnahmen. Insbesondere der Architektur ist ein ausgiebiges Kapitel gewidmet, da sie Basis für die Richtlinien, Konzepte und Maßnahmen ist. Berücksichtigung finden prozessuale, ressourcenspezifische und organisatorische Aspekte. Zu den behandelten Themen gehören u. a. Datensicherung, Firewalls, Identitäts- und Accessmanagement, Intrusion-Prevention-Systeme, Virens Scanner und biometrische Systeme. Entsprechend der pyramidenförmigen Darstellung nimmt der Umfang und Detaillierungsgrad in der Praxis von Ebene zu Ebene zu. Es folgt die Darstellung des IT-Lebenszyklus. Kapitel 14 enthält die Erläuterung des Sicherheitsregelkreises.

*Kapitel 6-14:
Elemente der
Sicherheits-
pyramide*

Kapitel 15 erläutert Reifegradmodelle und insbesondere das vom Autor konzipierte Reifegradmodell der Sicherheit, mit dem sich der Leser einen ersten Überblick über den Reifegrad des Sicherheitsmanagements im eigenen Unternehmen verschaffen kann.

*Kapitel 15:
Reifegradmodell
des Autors*

Kapitel 16 beschreibt – ausgehend von der Sicherheitspyramide – den vom Autor konzipierten Sicherheitsprozess bzw. Sicherheitsmanagementprozess oder auch Sicherheits-, Kontinuitäts- und Risikomanagementprozess, durch den das Sicherheits-, Kontinuitäts- und Risikomanagement geplant, aufgebaut, betrieben, geprüft, weiterentwickelt und am Leben gehalten wird.

*Kapitel 16:
Sicherheits-
management-
prozess des
Autors*

Kapitel 17 führt in einer Checkliste Basiselemente zu wichtigen Sicherheitseckpunkten auf.

*Kapitel 17:
Minimale
Sicherheit*

Den Abschluss des Buchs bilden das Abbildungs- und Markenverzeichnis, das Verzeichnis über Gesetze, Vorschriften, Standards und Normen sowie das Literatur- und Quellenverzeichnis. Nach dem Glossar und Abkürzungs- sowie dem Sachwortverzeichnis folgen im letzten Kapitel Informationen über den Autor.

*Gesetze,
Normen,
Literatur,
Glossar,
Sachwörter*

*Generisches
Maskulinum*

In diesem Buch verwendet der Autor ausschließlich aus Gründen der besseren Lesbarkeit das generische Maskulinum, d. h. die männliche Form, auch wenn beide Geschlechter gemeint sind.

*Struktur
der Kapitel:
Einführung,
Unterkapitel,
Hilfsmittel,
Praxisbeispiele,
Zusammen-
fassung*

Welche Struktur haben die Kapitel?

Die Kapitel enthalten – sofern sinnvoll – eine Einführung und einleitende Darstellung der jeweils folgenden Unterkapitel. Im Anschluss an die thematischen Beschreibungen in den Unterkapiteln folgen verschiedentlich praxisorientierte Hilfsmittel, z. B. Checklisten und Vorgehenselemente, die den erstmaligen Aufbau unterstützen und zum Gegencheck bei bereits etablierten Sicherheitsmanagementsystemen dienen können. Verschiedene aus der und für die Praxis angepasste Beispiele veranschaulichen die jeweilige Thematik. Eine Zusammenfassung bildet den Abschluss insbesondere größerer Kapitel.

*Abbildungen
und Tabellen*

Abbildungen und Tabellen visualisieren und strukturieren die Texte und machen sie transparent.

Was bedeuten die Piktogramme?



Dieses Symbol kennzeichnet Informationen, die z. B. aus der Presse stammen.



Abschnitte, in denen Erlebnisse des Autors dargestellt sind, hebt dieses Zeichen hervor. Erlebnisse dienen der Illustration der jeweiligen Kapitel und stellen den Praxisbezug her.



Dieses Zeichen macht Tipps kenntlich.

Was war neu in der 2. Auflage?

Gegenüber der ersten Auflage des Buchs „IT-Sicherheit mit System“ vom Mai 2003, das Ende Juli 2003 erschienen ist, wurde die zweite Auflage aktualisiert und deutlich erweitert. Neu hinzugekommen waren dort insbesondere folgende Themen:

- Ingenieurmäßige Sicherheit (Safety and Security Engineering)
- Ressourcen, Schutzobjekte und –subjekte sowie –klassen
- Geschäftskontinuität (Business Continuity)
- 10 Schritte zum Sicherheitsmanagement
- das Konformitäts-, Risiko-, Ereignis-, Wartungs-, Architektur-, Innovations- und Identitätsmanagement sowie das Patch- als Teil des Änderungsmanagements und der USB-Token
- der Sicherheitsprozess bzw. Sicherheitsmanagementprozess.

Erweitert wurden u. a.:

- die Sicherheitspyramide von der Version III zur Version IV
- der Risikodreiklang
- die Sicherheitspolitik zur Sicherheits- und Risikopolitik
- die Sicherheitsprinzipien
- das Leistungsmanagement um Sourcing und Provider-Management, ferner das Lizenz- und das Konfigurationsmanagement
- die Ausführungen zur Authentisierung und zu Firewalls
- das Glossar und Abkürzungsverzeichnis
- das Verzeichnis über Gesetze, Vorschriften, Standards, Normen.

Was ist neu in dieser 3. Auflage?

Gegenüber der zweiten Auflage des Buchs „IT-Sicherheit mit System“ vom April 2005, die im August 2005 erschienen ist, ist die vorliegende dritte Auflage an verschiedenen Stellen aktualisiert und in folgenden Themenfeldern deutlich erweitert worden:

- ITK-Sicherheitsmanagement (ISO 13335-1:2004, ISO 17799:2005, ISO 27001:2005, ISO 27002:2005, ITIL® Security Management, IT-Grundschutzhandbuch 2006, COBIT® 4.0, BS 25999-1:2006)
- Business-Safety-Security-Continuity-Risk-Alignment
- Externe Sicherheitsanforderungen einschließlich Sarbanes-Oxley Act und „EuroSOX“
- Ereignismanagement und Kennzahlen
- Architekturmanagement (biometrische Systeme, serviceorientierte Architektur, SOA, SOA Security, Web Services Security, SOAP, SAML, XACML, XKMS, Grid Computing, Grid Security, Kontrollen/Kontrollelemente (Controls))
- Sicherheitsrichtlinien
- Lebenszyklus (erweiterte Sicherheitselemente im Entwicklungsprozess)
- Reifegradmodelle
- Glossar, u. a. Botnet, CHAP, DLM, DNS, DRM, EICAR, eTAN, Fingerprinting, IMAP, iTAN, IT-Compliance, JCE, JSSE, Key-Logger, Konformität, LDAP, mTAN, OASIS™, PAP, Pharming, Phishing, POP, RADIUS, SAS No. 70, SQL-Injektion, TLS, VoIP, XSS

Wem sage ich Dank?

*Familie
Müller*

Auch diese Auflage entstand an langen Abenden, an Wochenenden und in Urlauben. Von daher bedanke ich mich bei meiner Familie, deren Toleranz für einen viel beschäftigten Ehemann und Vater ich wieder einmal stark beanspruchte.

Meiner Frau, selbst Herausgeberin und Co-Autorin verschiedener Lexika und Bücher sowie Lektorin und Übersetzerin, danke ich erneut für wertvolle Hinweise.

Ich bedanke mich bei meinen zum einen germanistisch und geschichtlich studierten sowie zum anderen zeichnerisch-musikalisch bewanderten Eltern und ihrer erfolgreichen Förderung. Sie macht sich an vielen Stellen dieses Buchs positiv bemerkbar.

Meinen Geschwistern danke ich für ihre Unterstützung.

*Lektorat
Vieweg-IT*

Dem Lektorat Vieweg-IT sage ich Dank und hier insbesondere Herrn Schulz für die Unterstützung bei der 3. Auflage, Herrn Dr. Klockenbusch für seine konstruktiven Hinweise und Vermarktungsideen zu den vorherigen Auflagen sowie Herrn Dapper, weil er mir vor der 1. Auflage den Anstoß gab, das Rohmanuskript zu einem Buch werden zu lassen.

ACG GmbH

Herrn G. Neidhöfer, Geschäftsführer der ACG Automation Consulting Group GmbH in Frankfurt, einer renommierten Unternehmensberatung, danke ich, weil er meine Ambitionen als Fachautor, die sich bisher in verschiedenen Artikeln und Büchern niedergeschlagen haben, stets unterstützt hat.

*Leser von
„IT-Sicherheit
mit System“*

Nicht zuletzt danke ich den vielen Lesern der vorherigen Auflagen, deren Feedback mich bestätigt sowie zu weiterem Schreiben angeregt hat, und zwar einerseits in Form dieser Neuauflage und andererseits in Form des „Handbuchs Unternehmenssicherheit“, das die Sicherheit der IT und des Unternehmens als Ganzes betrachtet. Nicht zuletzt Ihr Kaufinteresse hat den Verlag zu einer Neuauflage des vorliegenden Buchs motiviert. (*Am Rande bemerkt: Heißt es eigentlich motivieren „zu“ oder „für“ oder ist beides möglich? Die Antwort finden Sie vielleicht in dem einen oder anderen Wörterbuch und voraussichtlich ab 2008 oder 2009 in einem großvolumigen Welt-Unikat, dem Wörterbuch der deutschen Präpositionen von Dr. Wolfgang Müller, vorab vorgestellt in der Zeitschrift für germanistische Linguistik, 3/2004.*)

*Qualität und
Verbreitung der
Sicherheits-
pyramide*

Die Bezeichnung „Sicherheitspyramide“ wurde von mir Mitte der 90er Jahre des vorigen Jahrhunderts zusammen mit ihrer Darstellung veröffentlicht. Als Indiz für die Qualität und den Anklang meiner dreidimensionalen Sicherheitspyramide sowie meiner Artikel und

Bücher, so manches Mal sogar einer Vordenkerrolle, betrachte ich auch die seit jener Zeit und noch vermehrt nach Erscheinen meiner Bücher auftauchende Verwendung dieses Begriffs durch Dritte. Dies gilt ebenso für jene vereinzelt vorzufindenden Präsentationen und Grafiken Dritter, die eine bemerkenswerte strukturelle und/oder verbale Ähnlichkeit zur geschützten Darstellung meiner Sicherheitspyramide aufweisen. Ferner bezieht es sich auf Unterlagen und Darstellungen, die auf von mir geprägte Begriffe zurückgreifen. Zu finden sind sie in verschiedenen Publikationsmedien.

Als Bestätigung des Vorgehensmodells in Form der Sicherheitspyramide und deren Inhalten bzw. als Zeichen hoher Wertschätzung meiner Bücher und Publikationen sehe ich es an, dass sich Kernelemente und –methoden in Werken zur IT-Sicherheit wiederfinden. So manches Mal ist hierbei eine zeitliche Korrelation zwischen dem Erscheinen meiner Veröffentlichungen und dem anschließenden Auftauchen der darin vorgestellten Ideen, Ansätze, Begriffe, Hilfsmittel und Formulierungen feststellbar.

Sie finden in diesem Buch nur sehr begrenzt Zitate Dritter bzw. Textpassagen anderer Werke, dafür aber vielfältige Quellen- und verschiedene Markenangaben. Dies geschieht in Anerkennung der jeweiligen Leistung sowie in Achtung des Urheber- und Markenschutzes sowie des geistigen Eigentums und der Marken Dritter. Ich gehe davon aus und finde dies bei Profis und in Diplomarbeiten bestätigt, dass Leser meiner Bücher ebenfalls urheberrechtskonforme Quellenangaben verwenden. Für diese und mich gilt folgender Aphorismus nicht:

**Wer sich mit fremden Federn schmückt,
dem fehlen eigene.**
(kein asiatisches Sprichwort)

(29. April 2007, Dr.-Ing. Klaus-Rainer Müller)

Für die IT und ITK finden Sie das durchgängige und wegweisende Original der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller in diesem Buch und im „Handbuch Unternehmenssicherheit“. Letzteres ist Wegbereiter und Trendsetter für das Zusammenwachsen von IT- und Unternehmenssicherheit sowie von Sicherheits-, Kontinuitäts- und Risikomanagement. Es spricht neben diesen Themen außerdem externe Sicherheitsanforderungen durch Gesetze und Aufsichtsbehörden bis hin zu berufsgenossenschaftlichen Vorschriften an. Haben Sie es schon gelesen?

Wem ist dieses Buch gewidmet?

Für meine Familie, meine Eltern und Geschwister.

Was ist sicher?

Eins ist sicher: Nichts ist sicher.

(01. August 1998, Dr.-Ing. Klaus-Rainer Müller)

Was können Sie tun?

*Lesbarkeit und
Zielsetzung*

Ein weiterer für Sie wichtiger Aspekt ist die Lesbarkeit und Zielsetzung des Buchs. Ist das Buch eher wissenschaftlich trocken oder interessant lesbar und mit praktischen Beispielen und Tipps gewürzt?

Ich selbst habe mir vorgenommen, ein fundiertes und angemessen schlankes Buch zu schreiben, das praxisorientiert auf dem Modell der Sicherheitspyramide aufbaut, dabei einen wissenschaftlichen Beitrag zum Sicherheits-, Kontinuitäts- und Risikomanagement liefert und außerdem verständlich und leicht lesbar sowie zum Zeitpunkt der Manuskripterstellung aktuell ist. Ich hoffe, das ist mir mit dem vorliegenden Buch gelungen.

*Ihr
konstruktives
Feedback
ist gefragt*

Beurteilen werden dies letztendlich Sie, die Leser, auf deren konstruktive Kritik ich mich unter dem von meinem Vater, einem international renommierten Germanisten, in seinem Gegenwort-Wörterbuch angegebenen leicht abgewandelten Motto freue:

**Wenn Ihnen dieses Buch gefällt, sagen Sie es weiter,
wenn nicht, sagen Sie es mir.**

In diesem Sinne wünsche ich Ihnen eine spannende, interessante und weiterführende Lektüre.

Groß-Zimmern, im Juli 2007

Dr.-Ing. Klaus-Rainer Müller

Weitere Informationen des Autors finden Sie zum Zeitpunkt der Drucklegung unter www.bmsdm.de.

Inhaltsübersicht

1 Ausgangssituation und Zielsetzung.....	1
2 Kurzfassung und Überblick für Eilige	13
3 Zehn Schritte zum Sicherheitsmanagement.....	15
4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement ...	19
5 Die Sicherheitspyramide – Strategie und Vorgehensmodell.....	67
6 Sicherheits-, Kontinuitäts- und Risikopolitik.....	81
7 Sicherheitsziele / Sicherheitsanforderungen.....	97
8 Sicherheitstransformation.....	119
9 Sicherheitsarchitektur.....	129
10 Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte...	301
11 Spezifische Sicherheitskonzepte	341
12 Sicherheitsmaßnahmen	345
13 Lebenszyklus	347
14 Sicherheitsregelkreis.....	365
15 Reifegradmodell des Sicherheitsmanagements – Safety/Security/Continuity Management Maturity Model	383
16 Sicherheitsmanagementprozess.....	393
17 Minimalistische Sicherheit	401
Abbildungsverzeichnis.....	403
Markenverzeichnis	404
Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	405
Literatur- und Quellenverzeichnis	419
Glossar und Abkürzungsverzeichnis.....	425
Sachwortverzeichnis.....	475
Über den Autor.....	505

Inhaltsverzeichnis

1 Ausgangssituation und Zielsetzung	1
1.1 Ausgangssituation	2
1.1.1 Bedrohungen	2
1.1.2 Schwachstellen	6
1.1.3 Schutzbedarf	9
1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements	10
1.3 Lösung	10
1.4 Zusammenfassung	12
2 Kurzfassung und Überblick für Eilige	13
3 Zehn Schritte zum Sicherheitsmanagement	15
4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement	19
4.1 Unternehmenssicherheitsmanagementsystem	20
4.2 Informationssicherheitsmanagementsystem	21
4.3 Sicherheitsmanagement	22
4.4 ITK-Sicherheitsmanagement	23
4.4.1 ISO/IEC 13335-1:2004	24
4.4.2 ISO/IEC 17799:2005, ISO/IEC 27002:2005	26
4.4.3 ISO/IEC 27001:2005	28
4.4.4 ISO/IEC 27000-Reihe	30
4.4.5 ITIL® Security Management	31
4.4.6 IT-Grundschutzhandbuch, IT-Grundschutzkataloge des BSI	32
4.4.7 COBIT®, Version 4.0	37
4.4.8 BS 25999-1:2006	39
4.4.9 BS 25999-2	42
4.4.10 Fazit: Normen und Practices versus Sicherheitspyramide	43
4.5 Ingenieurmäßige Sicherheit – Safety, Security, Continuity Engineering	47
4.6 Sicherheitspyramide	47
4.7 Sicherheitspolitik	49
4.7.1 ... nach IT-Grundschutzhandbuch/-katalogen (IT-GSHB 2006)	49
4.7.2 ... nach ITSEC	50
4.7.3 ... nach ISO/IEC 13335-1:2004	51
4.7.4 ... nach ISO 15408 (Common Criteria)	52
4.7.5 ... nach ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005	52
4.7.6 ... nach ISO/IEC 27001:2005	53
4.7.7 ... nach Dr.-Ing. Müller	53
4.7.8 Vergleich	54
4.8 Sicherheit im Lebenszyklus	55

4.9 Ressourcen, Schutzobjekte und -subjekte sowie -klassen	56
4.10 Sicherheitskriterien.....	57
4.11 Geschäftseinflussanalyse (Business Impact Analysis).....	58
4.12 Geschäftskontinuität (Business Continuity)	58
4.13 Sicherheit und Sicherheitsdreiklang	61
4.14 Risiko und Risikodreiklang.....	63
4.15 Risikomanagement	65
4.16 Zusammenfassung	65
5 Die Sicherheitspyramide – Strategie und Vorgehensmodell	67
5.1 Überblick.....	68
5.2 Sicherheitshierarchie	72
5.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik	73
5.2.2 Sicherheitsziele / Sicherheitsanforderungen.....	73
5.2.3 Sicherheitstransformation	73
5.2.4 Sicherheitsarchitektur	74
5.2.5 Sicherheitsrichtlinien.....	74
5.2.6 Spezifische Sicherheitskonzepte.....	74
5.2.7 Sicherheitsmaßnahmen.....	75
5.3 PROSim	75
5.4 Lebenszyklus von Prozessen, Ressourcen, Produkten und Leistungen (Services)	76
5.4.1 Geschäfts-, Support- und Begleitprozess-Lebenszyklus	76
5.4.2 Ressourcen-/Systemlebenszyklus.....	77
5.4.3 Dienstleistungs- und Produktlebenszyklus.....	77
5.5 Sicherheitsregelkreis	77
5.6 Sicherheitsmanagementprozess	78
5.7 Zusammenfassung	78
6 Sicherheits-, Kontinuitäts- und Risikopolitik.....	81
6.1 Zielsetzung	82
6.2 Umsetzung	82
6.3 Inhalte	83
6.4 Checkliste.....	85
6.5 Praxisbeispiele.....	87
6.5.1 Sicherheits-, kontinuieräts- und risikopolitische Leitsätze Versicherung	87
6.5.2 Sicherheits-, Kontinuitäts- und Risikopolitik	89
6.6 Zusammenfassung	96
7 Sicherheitsziele / Sicherheitsanforderungen.....	97
7.1 Schutzbedarfsklassen	98
7.2 Schutzbedarfsanalyse.....	98
7.2.1 Prozessarchitektur und Prozesscharakteristika	99

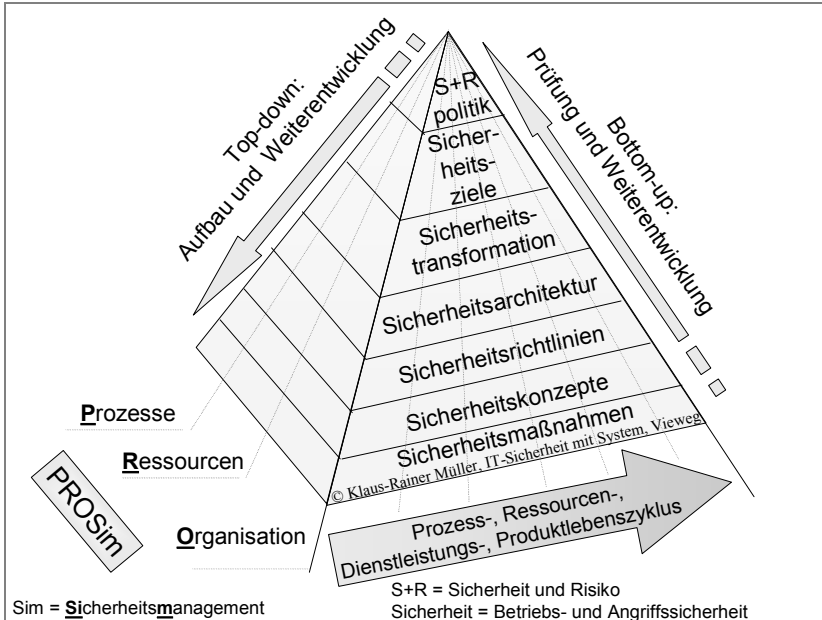
7.2.2 Externe Sicherheitsanforderungen	100
7.2.3 Geschäftseinflussanalyse (Business Impact Analysis)	108
7.2.4 Betriebseinflussanalyse (Operational Impact Analysis)	110
7.3 Tabelle Schadensszenarien	111
7.4 Praxisbeispiele	113
7.4.1 Schutzbedarf der Geschäftsprozesse	113
7.4.2 ITK-Schutzbedarfsanalyse	113
7.4.3 Schutzbedarfsklassen	117
7.5 Zusammenfassung	118
8 Sicherheitstransformation	119
8.1 Haus zur Sicherheit – House of Safety, Security and Continuity (HoSSC)	120
8.2 Safety, Security and Continuity Function Deployment (SSCFD)	121
8.2.1 Transformation der Anforderungen auf Sicherheitscharakteristika	121
8.2.2 Detaillierung der Sicherheitscharakteristika	123
8.2.3 Abbildung der Charakteristika auf den Lebenszyklus	123
8.3 Schutzbedarfsklassen	124
8.4 Praxisbeispiele	125
8.5 Zusammenfassung	127
9 Sicherheitsarchitektur	129
9.1 Überblick	130
9.2 Prinzipielle Sicherheitsanforderungen	132
9.3 Prinzipielle Bedrohungen	132
9.4 Strategien und Prinzipien	135
9.4.1 Risikostrategie (Risk Strategy)	137
9.4.2 Sicherheitsstrategie (Safety, Security and Continuity Strategy)	138
9.4.3 Prinzip der Wirtschaftlichkeit	139
9.4.4 Prinzip der Abstraktion	139
9.4.5 Prinzip der Klassenbildung	140
9.4.6 Poka-Yoke-Prinzip	140
9.4.7 Prinzip der Namenskonventionen	142
9.4.8 Prinzip der Redundanz (Principle of Redundancy)	142
9.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy)	145
9.4.10 Prinzip des „gesperrten“ Bildschirms (Clear Screen Policy)	145
9.4.11 Prinzip der Eigenverantwortlichkeit	145
9.4.12 Vier-Augen-Prinzip (Confirmed Double Check Principle)	146
9.4.13 Prinzip der Funktionstrennung (Segregation of Duties)	146
9.4.14 Prinzip der Sicherheitsschalen (Security Shells)	146
9.4.15 Prinzip der Pfadanalyse	147
9.4.16 Prinzip des generellen Verbots (Deny All Principle)	147
9.4.17 Prinzip der minimalen Rechte (Need to Use Principle)	147
9.4.18 Prinzip der minimalen Dienste	147

9.4.19	Prinzip der minimalen Nutzung.....	148
9.4.20	Prinzip der Nachvollziehbarkeit und Nachweisbarkeit	148
9.4.21	Prinzip des „sachverständigen Dritten“	148
9.4.22	Prinzip des Closed-Shop-Betriebs und der Sicherheitszonen	148
9.4.23	Prinzip der Prozess-, Ressourcen- und Lebenszyklusimmanenz	149
9.4.24	Prinzip der Konsolidierung	150
9.4.25	Prinzip der Standardisierung (Principle of Standardization)	151
9.4.26	Prinzip der Plausibilisierung (Principle of Plausibleness).....	151
9.4.27	Prinzip der Konsistenz (Principle of Consistency)	152
9.4.28	Prinzip der Untergliederung (Principle of Compartmentalization).....	152
9.4.29	Prinzip der Vielfältigkeit (Principle of Diversity)	153
9.5	Sicherheitselemente.....	153
9.5.1	Prozesse im Überblick.....	154
9.5.2	Konformitätsmanagement (Compliance Management).....	165
9.5.3	Datenschutzmanagement (Privacy Management).....	166
9.5.4	Risikomanagement (Risk Management)	168
9.5.5	Leistungsmanagement (Service Level Management).....	172
9.5.6	Finanzmanagement (Financial Management)	176
9.5.7	Projektmanagement (Project Management).....	177
9.5.8	Qualitätsmanagement (Quality Management).....	177
9.5.9	Ereignismanagement (Incident Management)	178
9.5.10	Problemmanagement (Problem Management)	184
9.5.11	Änderungsmanagement (Change Management).....	185
9.5.12	Releasemanagement (Release Management).....	188
9.5.13	Konfigurationsmanagement (Configuration Management).....	188
9.5.14	Lizenzmanagement (Licence Management)	189
9.5.15	Kapazitätsmanagement (Capacity Management).....	190
9.5.16	Wartungsmanagement (Maintenance Management).....	192
9.5.17	Kontinuitätsmanagement (Continuity Management)	193
9.5.18	Securitymanagement (Security Management)	211
9.5.19	Architekturmanagement (Architecture Management).....	246
9.5.20	Innovationsmanagement (Innovation Management).....	259
9.5.21	Personalmanagement (Human Resources Management).....	261
9.5.22	Ressourcen im Überblick.....	265
9.5.23	ITK-Hard- und Software	265
9.5.24	Infrastruktur	295
9.5.25	Dokumente	297
9.5.26	Personal.....	297
9.5.27	Organisation im Überblick.....	297
9.5.28	Lebenszyklus im Überblick.....	298
9.6	Hilfsmittel Sicherheits- und Risikoarchitekturmatrix	298
9.7	Zusammenfassung	300

10 Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte ...	301
10.1 Übergreifende Richtlinien.....	302
10.1.1 Sicherheitsregeln.....	302
10.1.2 Prozessvorlage.....	303
10.1.3 IT-Benutzerordnung.....	305
10.1.4 E-Mail-Nutzung.....	307
10.1.5 Internet-Nutzung.....	310
10.2 Betriebs- und Begleitprozesse (Managementdisziplinen).....	311
10.2.1 Kapazitätsmanagement.....	311
10.2.2 Kontinuitätsmanagement.....	313
10.2.3 Securitymanagement.....	325
10.3 Ressourcen.....	337
10.3.1 Zutrittskontrollsystem.....	337
10.3.2 Passwortspezifische Systemanforderungen.....	337
10.3.3 Wireless LAN.....	338
10.4 Organisation.....	339
10.5 Zusammenfassung.....	340
11 Spezifische Sicherheitskonzepte	341
11.1 Prozesse.....	342
11.1.1 Kontinuitätsmanagement.....	342
11.2 Ressourcen.....	343
11.2.1 Betriebssystem.....	343
11.3 Zusammenfassung.....	343
12 Sicherheitsmaßnahmen	345
12.1 Ressourcen.....	345
12.1.1 Betriebssystem: Protokoll Passworteinstellungen.....	345
12.2 Zusammenfassung.....	346
13 Lebenszyklus	347
13.1 Beantragung.....	348
13.2 Planung.....	349
13.3 Fachkonzept, Anforderungsspezifikation.....	349
13.4 Technisches Grobkonzept.....	350
13.5 Technisches Feinkonzept.....	351
13.6 Entwicklung.....	354
13.7 Integrations- und Systemtest.....	356
13.8 Freigabe.....	357
13.9 Software-Evaluation.....	357
13.10 Auslieferung.....	358
13.11 Abnahmetest und Abnahme.....	358

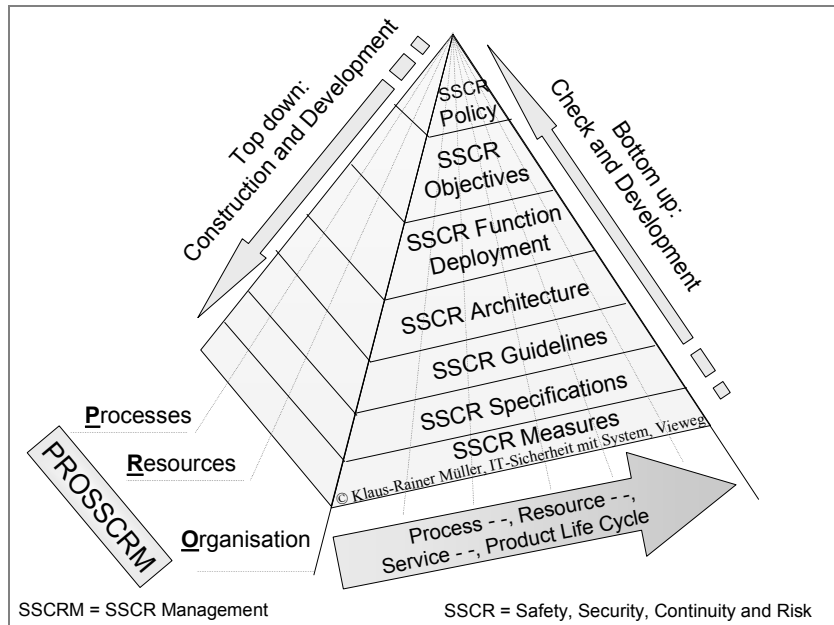
13.12 Software-Verteilung	359
13.13 Inbetriebnahme	360
13.14 Betrieb	360
13.15 Außerbetriebnahme	361
13.16 Hilfsmittel Phasen-Ergebnistypen-Tabelle	362
13.17 Zusammenfassung	363
14 Sicherheitsregelkreis	365
14.1 Sicherheitsprüfungen.....	366
14.1.1 Sicherheitsstudie/Risikoanalyse	366
14.1.2 Penetrationstests	370
14.1.3 IT-Security-Scans	371
14.2 Sicherheitscontrolling	372
14.3 Berichtswesen (Safety-Security-Reporting).....	374
14.3.1 Anforderungen	374
14.3.2 Inhalte	377
14.4 Safety-Security-Benchmarks	380
14.5 Hilfsmittel IT-Sicherheitsfragen	380
14.6 Zusammenfassung	381
15 Reifegradmodell des Sicherheitsmanagements – Safety/Security/Continuity Management Maturity Model	383
15.1 Systems Security Engineering – Capability Maturity Model®	384
15.2 Information Technology Security Assessment Framework.....	385
15.3 Security-Maturity-Modell.....	386
15.4 Reifegradmodell nach Dr.-Ing. Müller	386
15.4.1 Stufe 0: unbekannt.....	386
15.4.2 Stufe 1: begonnen	387
15.4.3 Stufe 2: konzipiert.....	387
15.4.4 Stufe 3: standardisiert	387
15.4.5 Stufe 4: integriert	388
15.4.6 Stufe 5: gesteuert.....	388
15.4.7 Stufe 6: selbst lernend	388
15.5 Checkliste Reifegrad.....	388
15.6 Praxisbeispiel	390
15.7 Zusammenfassung	391
16 Sicherheitsmanagementprozess.....	393
16.1 Deming- bzw. PDCA-Zyklus.....	393
16.2 Planung.....	394
16.3 Durchführung.....	396
16.4 Prüfung	396
16.5 Verbesserung.....	397

16.6 Zusammenfassung.....	397
17 Minimalistische Sicherheit	401
Abbildungsverzeichnis	403
Markenverzeichnis	404
Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices.....	405
Deutsche Gesetze und Verordnungen.....	405
Österreichische Gesetze und Verordnungen	406
Schweizer Gesetze, Verordnungen und Richtlinien	406
Britische Gesetze, Verordnungen und Richtlinien.....	407
Europäische Richtlinien	407
US-amerikanische Gesetze, Verordnungen und Richtlinien	408
Ausführungsbestimmungen, Grundsätze, Vorschriften	409
Standards, Normen, Leitlinien und Rundschreiben	410
Literatur- und Quellenverzeichnis	419
Glossar und Abkürzungsverzeichnis.....	425
Sachwortverzeichnis.....	475
Über den Autor	505



**Sicherheitspyramide IV nach Dr.-Ing. Müller bzw.
Sicherheitsmanagementpyramide IV nach Dr.-Ing. Müller**

Anmerkung: Sicherheit beinhaltet Betriebs- und Angriffssicherheit
sowie Kontinuität,
die Sicherheitspyramide umfasst Sicherheit und Risiko



Safety, Security, Continuity and Risk Pyramid IV
according to Dr.-Ing. Müller or
Safety, Security, Continuity and Risk Management Pyramid IV
according to Dr.-Ing. Müller

1 Ausgangssituation und Zielsetzung

Aufgrund der zunehmenden Vernetzung, der Globalisierung, des technologischen Fortschritts und des breiteren Allgemeinwissens steigen die Bedrohungen kontinuierlich an. Die IT, früher eine Wissenschaft für sich und wenigen Experten vorbehalten, gehört heute zum Schul- und Arbeitsalltag. Die Einstiegsbarriere für potenzielle Angreifer ist dementsprechend gering: Ein gebrauchter Computer, eine Anbindung an das Internet und entsprechendes Know-how und schon kann von fast jedem Punkt der Erde ein Angriff gefahren werden. Der Reiz mag darin liegen, dass jeder „David“ einen „Goliath“ zu Fall oder zumindest ins Stolpern oder Wanken bringen kann. Und Anlässe gibt es genug: (politische) Meinungsverschiedenheiten, (vermeintlich oder tatsächlich) „ungerechte“ Behandlung etc.

Bedrohungen

Früheren Software-Monolithen stehen heute komponentenbasierte Softwarepakete mit dynamischen Bibliotheken und Plug-ins gegenüber, umfangreich und hoch komplex. Die firmeninterne und -übergreifende Vernetzung von Informationssystemen bis hin zu weltweit verteilten Web-Services und weltumspannenden Grids, Remote-Access sowie die drahtgebundene und drahtlose Anbindung von PCs und Notebooks heben die Komplexität in eine neue Dimension. Dadurch steigt die Anzahl potenzieller Schwachstellen.

Schwachstellen

Durch gesetzliche und aufsichtsbehördliche Vorgaben, die wachsende Unterstützung der Geschäftsprozesse durch Computersysteme und die damit verbundene Abhängigkeit nehmen der Schutzbedarf der Unternehmen und die Haftungsrisiken der Verantwortlichen zu. Um mit diesen Entwicklungen Schritt zu halten, sind kontinuierlich zielgerichtete Investitionen in den Aufbau und die Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements erforderlich. Deren Umfang ist abhängig von den Anforderungen sowie der Effizienz und Effektivität des Sicherheits-, Kontinuitäts- und Risikomanagements. Die folgenden Unterkapitel informieren Sie über

*Schutzbedarf
und Haftung*

1. Ausgangssituation
2. Zielsetzung
3. Lösung
4. Zusammenfassung

1.1 Ausgangssituation

Wie sieht die derzeitige Risikolage aus? – Hierzu beschreiben die folgenden Unterkapitel die drei Komponenten des Risikos: die Bedrohungslage, aktuelle Schwachstellen und den Schutzbedarf.

1.1.1 Bedrohungen

Bedrohungen der IT ergeben sich in vielerlei Hinsicht: Erdbeben, Wassereintrich (z. B. Regen-, Fluss-, Grund- oder Leitungswasser), Brand oder Einbruch in Rechenzentren oder Technikräume, Ausfall der Stromversorgung oder der Kommunikationsanbindung, Fehlbedienung und Software-Fehler, aber auch Computerviren, Denial-of-Service-Attacken und Spionage.

Im Folgenden sind Ereignisse und Studien aus jüngerer Vergangenheit angegeben, welche die Vielfalt, das Vorhandensein und die Auswirkungen von Bedrohungen veranschaulichen.



Ausfälle und Bedrohungen

Stromausfälle: Am Donnerstag, den 14. August 2003, fällt im Nordosten der Vereinigten Staaten und in Kanada kurz nach 16:00 Uhr das Stromnetz in weiten Bereichen aus. Davon betroffen sind mehr als 50 Millionen Menschen. Am frühen Freitag Morgen, 14 Stunden danach, verfügen erst ein Viertel der Bewohner New Yorks wieder über Strom. [Frankfurter Allgemeine Zeitung (FAZ), 16.08.2003, S. 1]

Ende August 2003 legt ein Stromausfall in London 60 % des städtischen U-Bahnnetzes sowie 250 Ampel- und Signalanlagen lahm und verursacht ein Verkehrschaos. [FAZ, 12.9.2003, S. 18]

Am Dienstag, den 23. September 2003, fällt nachmittags in Teilen Dänemarks und Südschwedens der Strom aus. Etwa 4 Millionen Menschen sind davon betroffen und zum Teil für Stunden ohne Strom. Ampeln fallen aus und es kommt zu einem Verkehrschaos. Aufzüge und U-Bahnen bleiben stecken, das Telefonnetz ist zeitweilig unterbrochen und zahlreiche Unternehmen müssen die Produktion einstellen. [FAZ, 24.9.2003, S. 9]

Am frühen Sonntag Morgen, dem 28. September 2003, fällt in Italien landesweit der Strom aus. Die Rückwirkungen auf das deutsche Stromnetz wurden durch die sofortige Inbetriebnahme von Pumpspeicherwerken beherrscht. [FAZ, 29.9.2003, S. 9]

Nach Angaben der Energiekonzerne und anderer Fachleute ist ein solcher flächendeckender Stromausfall wie in Nordamerika in Deutschland nicht möglich. Die Städtischen Werke Magdeburg geben für deutsche Stromkunden einen Stromausfall von durchschnittlich 15 Minuten an. [FAZ, 16.08.2003, S. 11]

Aufgrund von Schneefall, eisiger Kälte und Wind fällt Ende November 2005 im Münsterland die Stromversorgung für mehrere Tage aus. Um Überland-Starkstromleitungen haben sich teilweise oberarmdicke Eispanser gelegt. Aufgrund ihres Gewichts in Kombination mit starkem Wind knicken 50 Hochspannungsmasten ein oder werden beschädigt. Licht, Heizung, Klima-, Alarm- und Telefonanlagen fallen aus. Schnee und umgestürzte Bäume bringen den Flug-, Bahn- und Straßenverkehr zeitweilig zum Erliegen. Die IHK Nord Westfalen schätzt, dass der Stromausfall bei Unternehmen einen wirtschaftlichen Schaden von mehr als 100 Millionen Euro verursacht hat. [FAZ, 28.11.2005 sowie 30.11.2005]

Ein Stromausfall in Münster am 9. Juni 2006 und ein „nach den inzwischen vorliegenden Erkenntnissen defektes Schaltrelais“ führen bei einem IT-Dienstleister zu einem Totalausfall seines Rechenzentrums. Alle angeschlossenen 470 Volks- und Raiffeisenbanken sind davon betroffen. Der Aufsichtsrat des IT-Dienstleisters entbindet den Entwicklungs- und Produktionsvorstand am 17. Juni 2006 seiner Aufgaben und stuft den Vorstandsvorsitzenden zum Vorstandsmitglied herab. [FAZ, 30.6.2006]

Mobilfunknetz-Ausfall: Am Donnerstag, den 4. September 2003, fällt im Großraum Frankfurt das Netz eines Mobilfunk-Providers für fast 14 Stunden aus, als neue Software auf den Vermittlungsrechner gespielt wurde. [Darmstädter Echo, 6.9.2003, S. 4]

Ausfall von Dienstleistern: Im Februar 2006 meldet das größte deutsche Geldtransportunternehmen Insolvenz an. Die Deutsche Bundesbank weist daraufhin ihre Filialen an, die Bargeldversorgung zu gewährleisten, gegebenenfalls durch flexible Öffnungszeiten. [FAZ, 21.2.2006]

Hochwasser: Im August 2002 verursacht das Hochwasser an Elbe und Mulde Millionenschäden. Stromnetze brechen zusammen, Rechenzentren von Unternehmen und Behörden werden überflutet und fallen aus.

Epidemien: Als Anfang 2006 erkennbar ist, dass sich die Vogelgrippe weltweit ausbreitet und potenziell die Möglichkeit der Ansteckung von Menschen besteht, entwickeln verschiedene Banken in Deutschland und England Notfallpläne. [FAZ, 11.1.2006, S. 18]

Feuer: Ein Brand im Rechenzentrum des deutschen Bundestages führt am Mittag des 5. Juli 2007 zur Abschaltung des zentralen Rechners. Ursache ist ein durchgeschmortes Kabel, das die Sprinkleranlage auslöste. Auch am Abend ist die IT noch nicht verfügbar. [www.handelsblatt.com, 6.7.2007, 9:56]

Computerkriminalität: Laut polizeilicher Kriminalstatistik 2006 (PKS 2006) der Bundesrepublik Deutschland, herausgegeben vom Bundeskriminalamt, nahm die Computerkriminalität im Jahr 2006 insgesamt leicht ab und zwar gegenüber 2005 um 4,9 % auf 59.149 erfasste Fälle. Gleichzeitig sank die Aufklärungsquote von 48,1 % auf 47,1 %. Mit 27.347 erfassten Fällen an erster Stelle steht der Betrug mittels rechtswidrig erlangter Debitkarten mit PIN. Hier ist mit -15,2 % ein deutlicher Rückgang zu verzeichnen. An zwei-

ter Stelle und zunehmend folgt der Computerbetrug – §236a StGB – mit 16.211 erfassten Fällen und einer Zunahme von 2,1 % gegenüber 2005. Die Aufklärungsquote bei Computerbetrug ist geringfügig von 48,7 % auf 48,9 % gestiegen. Mit 78,9 % befinden sich beim Computerbetrug die meisten Tatverdächtigen in der Altersgruppe der Erwachsenen mit 21 Jahren und älter.

Computerattacken: Wie die Universität von Maryland auf ihrer Homepage am 7. Februar 2007 berichtet, erfolgt alle 39 Sekunden ein Angriff auf einen an das Internet angeschlossenen Computer, also durchschnittlich 1,5 Angriffe pro Minute. Dies ist das Ergebnis einer Studie der A. James Clark School of Engineering. In der überwiegenden Zahl der Angriffe handelte es sich um wenig erfahrene Hacker, die mittels automatisierter Skripte Wörterbuch-Attacken durchführten, um über „brute-force“-Attacken Benutzerkennungen und Passwörter zu knacken. Als Benutzerkennung versuchten es die Skripte mit „root“, das am häufigsten verwendet wurde, gefolgt von „admin“ sowie „test“, „guest“, „info“, „adm“, „mysql“, „user“, „administrator“ und „oracle“. Beim Erraten des Passwortes wurde in 43 % der Fälle einfach erneut die Benutzerkennung eingegeben. Weitere Versuche nutzten Variationen des Benutzernamens oder ergänzten ihn um 123. Auch Zahlenfolgen wie „123456“, „12345“, „1234“, „123“ sowie „password“, „passwd“, „test“ und „1“ wurden versucht. Nach einem erfolgreichen Angriff änderten Hacker Passwörter und schleusten Backdoor-Programme ein, um die Computer fernsteuern zu können.

Computerviren und Spam: Sophos entdeckte laut seinem „Security threat report 2007“ im Jahr 2006 über 41.000 Mal neue Schadsoftware. Hierbei führte der E-Mail-Wurm Mytob mit rund 30 % die Liste der Top-Ten-Schadsoftware-Familien an. Gemeinsam mit Varianten der E-Mail-Würmer Netsky, Sober und Zafi machten diese Würmer demzufolge 75 % der infizierten E-Mails aus. Gegenüber 2005 sank der Anteil infizierter E-Mails jedoch von 1:44 auf 1:337.

Dem Bericht zufolge stammen über 90 % aller Spam-Mails von korrumpierten Computern, so genannten Zombie-PCs. Den Messungen von Sophos zufolge sind US-Computer die größten Spam-Versender, gefolgt von chinesischen und südkoreanischen. Aus diesen Ländern stammt insgesamt mehr als 45 % der Spams.

Kosten durch Sicherheitsverletzungen: Gemäß dem „information security breaches survey 2006“ des englischen Ministeriums für Handel und Industrie vom April 2006 haben englische Unternehmen noch einen weiten Weg vor sich, um eine Sicherheitskultur aufzubauen. Rund 40 % der Unternehmen investieren demzufolge weniger als 1 % ihres IT-Budgets in Informationssicherheit. Die Gesamtkosten für das schlimmste Ereignis des Jahres 2006 einschließlich Geschäftsunterbrechung und personellem Aufwand beliefen sich auf durchschnittlich 8.000 £ bis 17.000 £. Bei großen Unternehmen lagen sie mit durchschnittlich 65.000 £ bis 130.000 £ noch deutlich höher.

Einer Studie bei europäischen Kleinunternehmen zufolge summiert sich der finanzielle Schaden aufgrund von Ausfallzeit infizierter PCs auf 22 Milliarden Euro. Je Virenattacke entstehen dabei durchschnittlich Kosten in Höhe von 5.000 Euro. [Network Associates®: Pressemitteilung „Neue Studie von Network Associates: Netzwerk-Viren werden für kleine Unternehmen in Europa zum finanziellen Problem, 29. März 2004]

Datendiebstahl: Computerhacker nutzen eine Sicherheitslücke bei einem amerikanischen Kartenprozessor aus und stehlen Daten von mehr als 40 Millionen Kreditkarteninhabern namhafter Kreditkartenunternehmen. [FAZ, 22.6.2005, S. 15].

Pharming: Eine Umfrage von „The Measurement Factory“ vom 24.10.2005 ergab, dass 84 % der 1,3 Millionen betrachteten DNS-Server durch eine Pharming-Attacke korumpiert werden könnten. DNS-Server übersetzen die alphanumerische Internetadresse (URL) in eine IP-Adresse. Durch eine Manipulation der Zuordnung von URL zu IP-Adresse mittels Pharming ließe sich eine Umleitung auf gefälschte Webseiten erreichen. [www.measurement-factory.com]

Phishing: Zu den großen Sicherheitsproblemen, die sich im Jahr 2007 fortsetzen, gehört auch das Phishing, bei dem Datendiebe versuchen, durch gefälschte E-Mails und Websites in den Besitz vertraulicher Daten zu gelangen, d. h. Daten „abzufischen“. Die Anti-Phishing Working Group (APWG) listete für den April 2006 insgesamt 11.121 Phishing-Sites. Vom März zum April 2007 erfolgte ein Anstieg von 20.871 auf 55.643 nach einem Peak von rund 37.440 im Oktober und November 2006. Den rapiden Anstieg führt APWG auf eine Änderung der Taktik von Phishing-Gruppen zurück, die jetzt eine Vielzahl von URLs für dieselbe Domain nutzen. [APWG, Phishing Activity Trends, Report for the Month of April, 2007]

Datenverluste: Durch Sicherheitslücken beim Transport gehen einem bekannten amerikanischen Paketdienst Computerbänder einer amerikanischen Großbank mit Informationen über 3,9 Millionen Kunden verloren. Die Daten umfassen Namen, Sozialversicherungsnummern, Kontonummern und Zahlungsverhalten. Mehrere ähnliche Fälle hatte es in Amerika bereits im Februar, April und Mai 2005 gegeben. [FAZ, 8.6.2005, S. 20]

Bruch des Datenschutzes: Ein amerikanischer Internetdienst veröffentlichte im Juli 2006 versehentlich das Suchverhalten von über 600.000 Mitgliedern. Angegeben wurden über 20 Millionen Suchbegriffe, die von den Mitgliedern im Zeitraum März bis Mai eingegeben worden waren und zum Teil sehr persönlicher oder intimer Natur waren, wie z. B. Krankheiten. Adressaten der Daten, die der Internetdienst auf einer separaten Internetseite darstellte, waren Hochschulforscher. Der Zugriff auf diese Seite war jedoch auch der Öffentlichkeit möglich. [FAZ, 23.8.2006, S. 14]

Fehlende Datenlöschung: Gebraucht gekaufte mobile Geräte, wie Smartphones und PDAs, enthalten oftmals vertrauliche Daten, z. B. Bankdaten und Steuerinformationen, Computer-Passwörter, persönliche und

geschäftliche Korrespondenz sowie Vertriebsinformationen bis hin zu medizinischen Daten des Nutzers. Dies ergab ein Test mit 10 gebrauchten mobilen Geräten, die über eBay gekauft worden waren. [Trust Digital, Pressemitiz, 30.8.2006]

Computer- und Anwendungsmängel: Nachdem der Handel der Tokioter Börse Anfang November 2005 für einen halben Tag unterbrochen war, offenbarte das Handelssystem TSE Anfang Dezember gravierende funktionale Defizite: Ein trotz vorheriger Alarmmeldung fehlerhaft eingegebener Verkaufsauftrag ließ sich nicht zurückziehen. Daraufhin nahm der Präsident der Tokioter Börse seinen Hut ebenso wie der operative Chef der Computerabteilung und der Senior Managing Director. [Darmstädter Echo, 21.12.2005]

Software-Änderungen: Am Donnerstag, den 23. September 2004, führt ein Fehler im Abfertigungssystem der Deutschen Lufthansa AG zu 33 Flugstreichungen. Wahrscheinliche Ursache ist ein Software-Update. Das Backup-System konnte nicht eingesetzt werden, weil bei ihm sonst die gleichen Fehler aufgetreten wären. [FAZ, 24.9.2004, S. 17]

Update: Beim spanischen Domainverwalter ESNIC stürzte Ende August 2006 um 15:15 Uhr während der regelmäßigen 8-stündlichen Aktualisierung der Internetadressen der Server für rund zwei Stunden ab. Damit konnte auf ungefähr 400.000 Websites mit der Endung „.es“ nicht mehr über den DNS-Server der ESNIC zugegriffen werden. [s. a. handelsblatt.com, 30.8.2006]

1.1.2 Schwachstellen

Trotz dieser kontinuierlich steigenden Bedrohungen und der hohen Bedeutung des Sicherheits-, Kontinuitäts- und Risikomanagements zeigen sich oftmals markante Unzulänglichkeiten bei der Sicherheit und Risikolage der Unternehmen. Einen auszugsweisen Überblick geben die folgenden Unterkapitel.

1.1.2.1 Fehlende oder unklare Anforderungen

*Fehlende
Sicherheitsziele*

Sicherheitsschwerpunkte und -ziele des Unternehmens sind oftmals nicht oder nicht verbindlich definiert. Eine Vorgabe seitens des anfordernden Fachbereichs (Service-Nehmer) existiert häufig ebenfalls nicht, ebenso wenig ein standardisiertes Verfahren zur Ermittlung dieser Anforderungen.

*Fehlende
Anforderungen,
individuelle
Lösungen*

Die fehlenden Anforderungen führen zu individuellen Lösungen mit unterschiedlichem Sicherheitsniveau, die in der ITK des Öfteren durch den jeweils verantwortlichen ITK-Mitarbeiter (Service-Geber) und seine Erfahrungen geprägt werden. Dies hat nicht selten erhebliche Unterschiede im Sicherheitsniveau zur Folge, beispielsweise zwischen hostorientierter zentraler und seit langem etablierter Welt und

dezentraler Client-Server-Welt. Die Vernetzung von Systemen mit unterschiedlichem Sicherheitsniveau führt häufig zu einer Absenkung auf das niedrigste Niveau.

1.1.2.2 Unvollständiges Vorgehensmodell

Ein anschauliches und durchgängiges Vorgehensmodell, wie Sicherheits-, Kontinuitäts- und Risikomanagement im Unternehmen strategisch, systematisch, zielorientiert und effizient aufgebaut und weiterentwickelt werden soll, fehlt in Unternehmen des Öfteren. Hieraus ergeben sich unzureichende Transparenz und Nachvollziehbarkeit, Doppelarbeiten sowie Sicherheitslücken und Risiken.

*Fehlendes
umfassendes
und
durchgängiges
Vorgehens-
modell*

Letztere werden häufig erst dann behoben, wenn Sicherheitsverletzungen aufgetreten sind, d. h. „das Kind bereits in den Brunnen gefallen“ ist. Dieses reaktive Vorgehen führt verschiedentlich dazu, dass Sicherheitslücken kurzfristig symptomorientiert „gestopft“, anstatt langfristig ursachenorientiert und ganzheitlich behoben werden. Diese Defizite werden noch dadurch verstärkt, dass Unternehmen häufig keinen Ansatz dafür finden, wie sie eine gesamtheitliche und kostenadäquate Lösung entwickeln können.

*Reaktives
symptom-
orientiertes
Vorgehen*

Außerdem existiert kein Verfahren, wie das im Unternehmen vorhandene Know-how im Thema Sicherheits-, Kontinuitäts- und Risikomanagement ausreichend gesichert und gepflegt sowie allen Beteiligten zur Verfügung gestellt werden kann.

*Know-how-
Sicherung*

1.1.2.3 Fehlende Lebenszyklusorientierung

An die Sicherheit denken Projekt- und IT-Leiter häufig erst bei der Inbetriebnahme oder dem Betrieb eines Prozesses oder eines Informations- und Telekommunikationssystems (ITK-System). Dementsprechend spät werden Überlegungen angestellt, welche Sicherheitsanforderungen bestehen und welche Sicherheitsmaßnahmen ergriffen werden müssen. Hieraus ergeben sich in der Regel nachträgliche Änderungen, die mehr Kosten verursachen als bei einer frühzeitigen Bearbeitung.

*Späte
Sicherheits-
überlegungen*

Ursache für diese Defizite ist die Fokussierung auf den Betrieb. Prozesse, Produkte und (Informations-)Systeme besitzen jedoch einen Lebenszyklus. Bevor ein System in den Betrieb geht, muss die entsprechende Idee geboren worden sein, das Konzept erstellt sowie Entwicklung und Test durchgeführt worden sein. In diesen frühen Phasen des Lebenszyklus wird der Grundstein für die spätere Sicherheit gelegt.

*Fokussierung
auf den Betrieb*

1.1.2.4 Übermäßige Technologiefokussierung

Prozesse,
Ressourcen und
Organisation

Sicherheitsmaßnahmen werden oftmals nur unter dem Blickwinkel einsetzbarer Technologien betrachtet. Doch Technologien sind nur Mittel zum Zweck. Sie stellen einen Teilaspekt der Themenfelder dar, die zur Umsetzung der Sicherheitsanforderungen genutzt werden können. Ebenfalls zu betrachten sind die Themenfelder Prozesse, Ressourcen und Organisation. Hiermit können ganzheitliche und im Zusammenspiel effiziente Sicherheitslösungen geschaffen werden. Dies erfordert insbesondere, dass das Top Management seine Vorstellungen und Ziele artikulieren und die hierfür erforderlichen Mittel und Ressourcen bereitstellen muss. Dementsprechend müssen das Mittelmanagement und die Mitarbeiter sensibilisiert und geschult werden.



11. Sicherheitsstudie der <kes> 2006 [2]

In obiger Studie [2] wurde die Frage gestellt, welche Probleme bei der Verbesserung der Informationssicherheit am meisten behindern. Mit 55 % am häufigsten genannt wurde, dass es an Geld fehle. Auf den folgenden Plätzen wird angeführt, es fehle an Bewusstsein ...

... bei den Mitarbeitern	52 %
... und Unterstützung im Top Management	45 %
... beim mittleren Management	37 %

1.1.2.5 Unzureichende Standardisierung

Fehlende
Standardisie-
rung

Warum werden die Gliederungsstruktur und die prinzipiellen Inhalte eines Datensicherungs- oder Datenschutzkonzepts, die generellen Zugangs- und Zugriffsregeln in manchen Unternehmen jedes Mal „neu erfunden“? Warum ist die Qualität der jeweiligen Ergebnisse unterschiedlich? Weil vorhandene Konzepte nicht abstrahiert und zu übergreifenden Standards weiterentwickelt werden. Dadurch hängt das Sicherheitsniveau stark von den Vorkenntnissen der Mitarbeiter ab. So können beispielsweise verschiedene UNIX®- oder Windows®-NT®-Systeme aufgrund unterschiedlicher Systembetreuer ganz verschiedene Sicherheitsniveaus aufweisen.

Unternehmensspezifische Standards und Checklisten, die „nur“ system-, anwendungs- und plattformspezifisch angepasst werden müssen, schaffen hier Abhilfe.

Kostensparende
Standards

Standards können auch teure Fehlinvestitionen in solche Anwendungssysteme und Betriebssysteme vermeiden helfen, deren Sicherheitsniveau den Anforderungen von vornherein nicht entspricht.

Die systematische Sicherung vorhandenen Know-hows und der strukturierte Zugriff auf Regeln, Richtlinien, Standards oder Vorgaben können nicht nur die Qualität und Sicherheit der Ergebnisse erhöhen. Sie steigern auch die Effizienz ihrer Erstellung und senken damit die hierfür erforderlichen Zeiten und Kosten.

*Know-how-
Sicherung*

1.1.3 Schutzbedarf

Wie sieht es mit dem Schutzbedarf der Unternehmen aus? Die Unterstützung der Geschäftsprozesse durch Informationssysteme nimmt zu. Lieferanten und Kunden sind an die Informationssysteme angebunden, wie z. B. beim Onlinebanking oder Onlineshopping. Sie wollen und sollen Transaktionen „rund um die Uhr“ abwickeln können. Ausfälle verursachen daher hohe Kosten und Image-Schäden.

*Online für
Kunden und
Lieferanten*

Ausfallkosten

Einer Onlineumfrage [3] von Contingency Planning Research zufolge, die im Jahr 2001 durchgeführt wurde, kostet ein einstündiger Computerausfall 54 % der teilnehmenden Unternehmen mehr als 51.000 Dollar. Bei 8 % sogar mehr als 1 Million Dollar.



Ausfallfolgen

Als der Netzzugang des Onlineauktionators eBay im Jahr 1999 für 22 Stunden blockiert war, ging der Börsenwert des Start-up-Unternehmens an einem einzigen Tag um 2,25 Milliarden Dollar ein [Computerwoche: Hardwarefehler zwingen IT-Systeme in die Knie, 27/2000, 07.07.2000].

Doch damit nicht genug. Auch der Gesetzgeber stellte neue Anforderungen. In Deutschland beispielsweise durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), durch das Teledienstegesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG), das Telemediengesetz (TMG), die Weiterentwicklung des Bundesdatenschutzgesetzes sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Im Bankenbereich hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Ende 2005 in einem Rundschreiben die Mindestanforderungen an das Risikomanagement (MaRisk) dargelegt und auch die „Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen“, kurz Basel II, des Baseler Ausschusses für Bankenaufsicht stellt neue Anforderungen. Im Mai 2006 verabschiedete das europäische Parlament die EuroSOX, die ähnlich wie der Sarbanes-Oxley-Act zusätzliche Anforderungen an Unternehmen stellt.

*Gesetze und
Regularien*

*Zunehmender
Schutzbedarf*

Dies zeigt, dass der Schutzbedarf nicht nur kontinuierlich angestiegen ist, sondern weiter wächst. Zunehmender Schutzbedarf bedeutet jedoch gleichzeitig wachsendes Risiko. Um dies zu reduzieren, müssen die Sicherheitsmaßnahmen kontinuierlich weiterentwickelt werden.

1.2 Zielsetzung des Sicherheits-, Kontinuitäts- und Risikomanagements

Das Sicherheits-, Kontinuitäts- und Risikomanagement muss demzufolge so aufgebaut sein, dass es der kontinuierlichen Zunahme der Bedrohungen Paroli bietet und dem steigenden Schutzbedarf Rechnung trägt, oder besser noch, ihn antizipiert. Wer für Sicherheit verantwortlich ist, sieht sich dementsprechend auch mit folgenden Anforderungen und Fragestellungen konfrontiert, die im Sicherheitsalltag immer wieder auftreten und bearbeitet sein wollen:

- Wie kann das Top Management für die Themen Sicherheits-, Kontinuitäts- und Risikomanagement sensibilisiert und darin eingebunden werden? – Wie wird es dazu motiviert, Vorgaben zu machen und sich an die Spitze des Sicherheits-, Kontinuitäts- und Risikomanagements zu stellen?
- Wie können die Mitarbeiter für die Themen Sicherheit, Kontinuität und Risiko sensibilisiert werden?
- Wie lassen sich die Sicherheits- und Kontinuitätsanforderungen der ITK-Nutzer erfassen?
- Welche Möglichkeiten gibt es, um das Sicherheits- und Kontinuitätsniveau zu definieren?
- Wie lassen sich die Anforderungen der ITK-Nutzer in entsprechende Sicherheitskonzepte und -maßnahmen überführen?
- Wie können Erkenntnisse, z. B. aus der Host-Welt, aber auch aus dezentralen Systemen, gesammelt, konsolidiert und allen Beteiligten verfügbar gemacht werden?
- Wie kann das Sicherheits-, Kontinuitäts- und Risikomanagementsystem gesteuert und kontinuierlich weiterentwickelt werden?

1.3 Lösung

*Allgemeines
3D-Pyramiden-
modell*

Vor diesem Hintergrund habe ich die dreidimensionale Sicherheitspyramide (3D-Sicherheitspyramide) entwickelt. Sie basiert auf dem allgemeinen bzw. generischen dreidimensionalen Pyramidenmodell nach Dr.-Ing. Müller, das jetzt in der Version IV vorliegt (s. Kapitel 5). Dieses eignet sich, wie bereits in [4] dargestellt wurde, für eine breite Palette

von Themenfeldern im organisatorischen und Managementbereich außerhalb und innerhalb der ITK. Es verkörpert ein systematisches, anschauliches und durchgängiges Vorgehens- und Organisationsmodell zum Aufbau und zur Weiterentwicklung praxisorientierter Managementsysteme. Beispiele hierfür sind die verschiedenen themenspezifischen Pyramiden des Autors, wie z. B. die Unternehmens-, die Kontinuitäts- bzw. BCM-, die ITK-Governance-, die Sourcing-, die IT-, die ITK-, die Unternehmenssicherheits-, die Sicherheits-, die IT-Sicherheits-[4], die Risiko-, die Qualitäts-, die Test-, die Projekt- und die Service-Pyramide bzw. jeweils –managementpyramide des Autors.

Die dreidimensionale Sicherheitspyramide dient als systematisches, verständliches und anschauliches Vorgehensmodell für den Aufbau und die Weiterentwicklung eines professionellen und integrativen Sicherheits-, Kontinuitäts- und Risikomanagements. Sie stellt eine Art Leitfaden oder „Kochbuch“ dar. Durch ihren top-down-orientierten stufenweisen Aufbau lassen sich die einzelnen Sicherheitselemente Schritt für Schritt entwickeln, in die Sicherheitspyramide „einklinken“ und weiter verfeinern. Einmal gewonnene Erkenntnisse können aufgenommen, für die Zukunft gesichert und anderen Mitarbeitern verfügbar gemacht werden. Gleichzeitig lassen sich Fehlinvestitionen vermeiden, indem zukünftige Systeme, wie z. B. Rechner und Anwendungen, vor ihrer Anschaffung auf ihre sicherheitstechnische Eignung überprüft werden und die Sicherheitsanforderungen in die Systemspezifikation einfließen.

*Drei-
dimensionale
Sicherheits-
pyramide*

Die Sicherheitspyramide lässt sich für die gesamte Palette von Sicherheitsthemen eines Unternehmens nutzen. In diesem Buch ist sie unter dem Fokus der IT- bzw. ITK-Sicherheit beschrieben.

Die erste Version der Sicherheitspyramide wurde von mir 1995 entwickelt und auf den Datensicherheitstagen [1] vorgestellt, die weiterentwickelte zweite Version 1996 in der Zeitschrift KES [5] veröffentlicht. Hier wie auch in weiteren Artikeln [6] [7] wurde von mir darauf hingewiesen, dass der gesamte Prozess der Softwareerstellung auch unter Berücksichtigung der Sicherheitskriterien zu betrachten ist. Diese Veröffentlichungen des Autors konzentrierten sich auf die Darstellung des hierarchischen Aufbaus der Sicherheitspyramide, auf Begleitprozesse und auf die Beschreibung des Software-Entwicklungsprozesses im Hinblick auf Sicherheit.

*Historie der
Sicherheits-
pyramide*

Das vorliegende Buch beschreibt alle drei Dimensionen der Version IV der dreidimensionalen Sicherheitspyramide des Autors. Die systematische Gliederung des Buchs orientiert sich zum einen an der ersten Dimension der Sicherheitspyramide, den hierarchischen Ebenen. Hierbei geht der Text auch ein auf die zweite Dimension mit den

*Drei-
dimensionale
Sicherheits-
pyramide IV*

IT-Prozessen, Ressourcen und der Organisation. Es folgt die dritte Dimension in Form des Lebenszyklus. Hieran schließen sich die Kapitel zum Sicherheitsregelkreis, zum Reifegradmodell und zum Sicherheitsmanagementprozess an.

1.4 Zusammenfassung

*Bedrohungen,
Schwachstellen
und
Schutzbedarf*

Die Bedrohungen für Unternehmen nehmen aufgrund der Vernetzung, Globalisierung und des technologischen Fortschritts sowie der geringen Einstiegsbarriere für potenzielle Angreifer kontinuierlich zu. Umfang und Komplexität der Informationssysteme steigen und mit ihnen die potenziellen und tatsächlichen Schwachstellen. Beispiele hierfür sind:

- unklare Sicherheitsanforderungen
- unvollständiges Vorgehensmodell
- fehlende Lebenszyklusorientierung
- übermäßige Technologiefokussierung
- unzureichende Standardisierung.

Durch die Onlineanbindung von Kunden und Lieferanten sind Unternehmen immer stärker auf die Funktionsfähigkeit ihrer Informationssysteme angewiesen.

Risikozunahme

Die Zunahme der Bedrohungen, der Schwachstellen und des Schutzbedarfs führen zu einem deutlichen Anstieg der Risiken. Diese haben Auswirkungen auf die Handlungsfähigkeit, das Image und die finanzielle Situation der Unternehmen. Gefordert ist daher ein anpassungsfähiges, effizientes und effektives Sicherheits-, Kontinuitäts- und Risikomanagement, das die Risiken auf ein wirtschaftlich vertretbares Maß reduziert.

*Sicherheits-
pyramide:
hierarchisch,
lebenszyklus-
orientiert,
ganzheitlich*

Hierzu dient die Sicherheitspyramide nach Dr.-Ing. Müller. Sie stellt ein anschauliches strategisches und systematisches Vorgehensmodell dar, ist hierarchisch aufgebaut und ermöglicht einen schrittweisen Aufbau bis hin zu einem integrativen Sicherheits-, Kontinuitäts- und Risikomanagement. Sie berücksichtigt den Lebenszyklus von Prozessen und Ressourcen, wie beispielsweise Systemen, sowie Produkten und Dienstleistungen. Die Themenfelder Prozesse, Ressourcen und Organisation im Hinblick auf das Sicherheitsmanagement, vom Autor PROSim genannt, werden ebenfalls betrachtet. Die Sicherheitspyramide erlaubt es, eine Sicherheitsstrategie zu entwickeln und Sicherheitselemente Schritt für Schritt aufzubauen, „einzuklinken“ und weiterzuentwickeln. Der Sicherheitsregelkreis ermöglicht die zielgerichtete Verfolgung und Steuerung des Sicherheits-, Kontinuitäts- und Risikomanagements.

2 Kurzfassung und Überblick für Eilige

Vorhandene Sicherheitskonzepte und -maßnahmen sind oft Inselösungen oder Ad-hoc-Maßnahmen mit unterschiedlichem Sicherheitsniveau. Darüber hinaus bestehen nicht selten hohe Abhängigkeiten vom Know-how der Mitarbeiter. Hieraus ergibt sich eine latente Bedrohung für die Existenz, die Handlungsfähigkeit und das Image eines Unternehmens.

Bedrohung der Handlungsfähigkeit

Um diesen Bedrohungen entgegenzuwirken, kann die dreidimensionale IT- bzw. ITK-Sicherheitspyramide nach Dr.-Ing. Müller eingesetzt werden. Sie bietet ein anschauliches, strukturiertes und strategisches Top-down-Vorgehensmodell zum ganzheitlichen Aufbau und zur zielgerichteten Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements. Sie beantwortet folgende Fragen:

Drei-dimensionale IT- bzw. ITK-Sicherheitspyramide

- Wie lassen sich ITK-Sicherheit sowie Kontinuität und Risiko an den Geschäftszielen ausrichten?
- Wie kann das Sicherheits-, Kontinuitäts- und Risikomanagement systematisch aufgebaut und weiterentwickelt werden?
- Welche Prozesse und Themen müssen berücksichtigt werden?
- Wie kann prozess-, ressourcen-, produkt-, leistungs- und lebenszyklusimmanente Sicherheit erreicht werden?
- Wie lässt sich die Sicherheit zielgerichtet weiterentwickeln?

Der systematische Aufbau des Sicherheitsmanagements zeigt sich in den sieben Hierarchieebenen der Sicherheitspyramide.

Systematischer Aufbau

Die oberste Ebene bildet die Sicherheits-, Kontinuitäts- und Risikopolitik des Unternehmens. In ihr stellt das Top Management dar, welche Bedeutung das Thema Sicherheit für das Unternehmen hat. Dies leitet sie ab von externen Vorgaben, der Unternehmenspolitik und der strategischen Positionierung des Unternehmens.

Sicherheits-, Kontinuitäts- und Risikopolitik

In der nächsten Ebene der Sicherheitspyramide definieren die Geschäftsprozess- und Bereichsverantwortlichen die Sicherheitsziele. Sie klassifizieren hierzu die Geschäfts- und Supportprozesse des Unternehmens nach ihrer Bedeutung. Über Schutzbedarfsanalysen ermitteln sie, welche Folgen Sicherheitsverletzungen nach sich ziehen können. Hieraus leiten sie die Sicherheitsanforderungen des jeweiligen Prozesses ab sowie der ihn unterstützenden ITK-Systeme. Entsprechend den Anforderungen, beschrieben aus der Sicht der Geschäfts- und Supportprozesse, erfolgt die Zuordnung in eine Sicherheitsklasse.

Sicherheitsziele

<i>Sicherheits- transformation</i>	Um die fachlichen Sicherheitsanforderungen zu erfüllen, muss die ITK entsprechende Maßnahmen ergreifen. Hierzu wandelt sie die fachlichen Anforderungen in prozessuale, ressourcenspezifische und organisatorische ITK-Sicherheitselemente um, die diese Anforderungen erfüllen. Diese Umsetzung bezeichnet der Autor als Sicherheits-transformation.
<i>Sicherheits- architektur</i>	Die nächste Ebene der Sicherheitspyramide enthält die Sicherheits-architektur. Sie beschreibt die prinzipiellen Sicherheitsanforderungen und Bedrohungen. Außerdem stellt sie die Sicherheitsstrategie und -prinzipien sowie die generellen Sicherheitselemente dar, die zur Umsetzung der Sicherheitsanforderungen und zum Schutz vor Be-drohungen vorhanden sind. Die Sicherheitselemente beziehen sich auf Prozesse, Prozesselemente, Ressourcen und Organisation.
<i>Sicherheits- richtlinien</i>	Um das Sicherheitsniveau zu vereinheitlichen und die Effizienz zu steigern, existiert die Ebene der plattformübergreifenden, aber unternehmensspezifischen Sicherheitsrichtlinien. Richtlinien legen z. B. fest, wie Prozessbeschreibungen sowie Notfall- und Katastrophen-vorsorgehandbücher strukturiert sind, wie E-Mails zu handhaben sind, welche Länge Passwörter haben sollen etc.
<i>Sicherheits- konzepte</i>	Die Sicherheitskonzepte bilden die Vorgaben der Sicherheitsricht-linien spezifisch auf die jeweilige Ressource, z. B. eine Plattform oder ein Informationssystem, oder den jeweiligen Prozess ab.
<i>Sicherheits- maßnahmen</i>	In der untersten Ebene, den Sicherheitsmaßnahmen, werden die Si-cherheitskonzepte realisiert und die Umsetzung dokumentiert.
<i>PRO und PROSim</i>	Die Frage nach den Themenfeldern, die im Sicherheitsmanagement zu behandeln sind, beantwortet die zweite Dimension der Pyramide. Sie beinhaltet die Themenfelder <u>P</u> rozesse, <u>R</u> essourcen und <u>O</u> rganisation (PRO) für das <u>S</u> icherheits <u>m</u> anagement, weshalb sie hier PRO-Sim heißt. PROSim ist in jeder Ebene der Sicherheitspyramide zu berücksichtigen.
<i>Lebenszyklus</i>	Die dritte Pyramidendimension dient der Integration der Sicherheits-thematiken in den Lebenszyklus von Prozessen, Produkten, (Infor-mations-)Systemen und Leistungen. So können Sicherheitsanfor-derungen bereits in einer sehr frühen Phase im Lebenszyklus berück-sichtigt und in den folgenden Phasen weiter verfeinert werden. Hier-aus ergibt sich schließlich eine lebenszyklus-, prozess- und damit produkt- sowie leistungs- und systemimmanente Sicherheit.
<i>Sicherheits- management- prozess, Regelkreis</i>	Der Sicherheitsprozess und der Regelkreis ermöglichen zielgerichtet die Planung, den Aufbau, die Steuerung und die Weiterentwicklung des Sicherheitsmanagements, um diesbezüglich Handlungsfähigkeit und Image eines Unternehmens langfristig zu sichern und zu steigern.

3 Zehn Schritte zum Sicherheitsmanagement

Sie wollen sofort mit dem Aufbau des Sicherheits-, Kontinuitäts- und Risikomanagements beginnen, ohne das Buch vorher komplett gelesen zu haben? Dann können Sie in folgenden 10 Schritten vorgehen, wobei Sie das jeweils dazugehörige Kapitel mit den dortigen Hilfsmitteln und Beispielen nutzen sowie die Umsetzungstipps im Anschluss an die folgende Tabelle.

Nr.	Aktivität	In Kapitel Sicherheits-...	Hilfsmittel	Beispiel
1.	Definition und Verabschiedung der Sicherheits-, Kontinuitäts- und Risikopolitik	..., Kontinuitäts- und Risikopolitik	Checkliste	Sicherheits-, Kontinuitäts- und Risikopolitik
2.	Erhebung der Sicherheitsanforderungen bzw. Sicherheitsziele	...-ziele/-anforderungen	Tabelle Schadensszenarien, Prozessinformationsdatenbank	Schutzbedarfsanalyse, Schutzbedarfsklassen
3.	Transformation der Sicherheitsanforderungen/-ziele auf Prozesse und Ressourcen	...-transformation	Safety, Security and Continuity Function Deployment	Praxisbeispiel
4.	Entwicklung der Sicherheitsarchitektur und -strategie	...-architektur	Prinzipielle Anforderungen, Sicherheitskriterien und Bedrohungen, Sicherheitsprinzipien und -elemente, Sicherheits-schalenmodell	Sicherheitsarchitekturmatrix

Nr.	Aktivität	In Kapitel Sicherheits-...	Hilfsmittel	Beispiel
5.	Entwicklung von Sicherheitsrichtlinien und -standards (generische Sicherheitskonzepte)	...-richtlinien	Sicherheitsregeln, Prozessvorlagen, verschiedene Richtlinien, Tätigkeiten-Rollen-Matrix	Beispiele
6.	Entwicklung spezifischer Sicherheitskonzepte	...-konzepte		Beispiele
7.	Umsetzung von Sicherheitsmaßnahmen	...-maßnahmen		Beispiel
8.	Integration der Sicherheit in den Lebenszyklus	Lebenszyklus	Phasen-Ergebnistypen-Tabelle	
9.	Aufbau des Sicherheitsregelkreises, Prüfung des Sicherheitsmanagements	...-regelkreis ...-regelkreis, Reifegradmodell	Sicherheitsregelkreis, Berichtswesen Sicherheitsstudie, Sicherheitsfragen, Checkliste Reifegrad	Reifegradmodell: Praxisbeispiel
10.	Etablierung des Sicherheitsmanagementprozesses	...-prozess	Tabelle mit Prozessschritten, Eingangsinformationen, Methoden und Ergebnissen	

Um Vorgehensfehler möglichst zu vermeiden, sollten Sie das jeweilige Kapitel lesen und die Inhalte anschließend auf Ihre Thematik angepasst umsetzen. Hierbei helfen Ihnen die Beispiele, Checklisten und Hilfsmittel.

Selbst kleine Unternehmen sollten alle hierarchischen Ebenen und die Dimensionen der Sicherheitspyramide sowie alle Elemente der Sicherheitsarchitektur lesen und auf Relevanz prüfen, da diese üblicherweise sowohl auf große und mittlere als auch auf kleine Unternehmen zutreffen. Nehmen wir als Beispiel das Kapazitäts- und das Lizenzmanagement. Fehlende Kapazität von IT-Systemen schränkt die Handlungsfähigkeit eines Unternehmens ein. Somit ist die Verfügbarkeit nicht mehr oder nur unzureichend gegeben. Fehlendes Lizenzmanagement kann zur Verletzung von Verträgen und Gesetzen führen. Im günstigsten Fall ist es aufgrund zu vieler Lizenzen nur unwirtschaftlich. Dies zeigt beispielhaft, dass auch weniger beachtete Sicherheitselemente für kleine Unternehmen erforderlich sind. Ihre Umsetzung gestaltet sich bei kleineren Unternehmen jedoch meist erheblich schlanker, indem auf Prozessbeschreibungen verzichtet werden kann und die entsprechenden Aufgaben „nur“ in die Stellenbeschreibung des jeweils Verantwortlichen und seines Stellvertreters aufgenommen werden.

*Umsetzungs-
tipps zum
Sicherheits-
management
für KMUs*

4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement

Begriffen werden oftmals unterschiedliche Bedeutungen zugeordnet. Um ein gemeinsames Verständnis zu den hier verwendeten spezifischen Fachbegriffen zu schaffen, enthalten die folgenden Unterkapitel diesbezügliche Erläuterungen. Im Kapitel Glossar und Abkürzungsverzeichnis finden Sie viele weitere Erklärungen. Sollten Sie darüber hinaus Stichwörter oder Abbildungen suchen, so helfen Ihnen das Sachwort- und das Abbildungsverzeichnis beim Finden.

Das vorliegende Kapitel erläutert in den folgenden Unterkapiteln diese Begriffe:

1. Unternehmenssicherheitsmanagementsystem
2. Informationssicherheitsmanagementsystem
3. Sicherheitsmanagement
4. ITK-Sicherheitsmanagement
5. Ingenieurmäßige Sicherheit
(Safety, Security and Continuity Engineering)
6. Sicherheitspyramide
7. Sicherheitspolitik
8. Sicherheit im Lebenszyklus
9. Ressourcen, Schutzobjekte und –subjekte sowie -klassen
10. Sicherheitskriterien
11. Geschäftseinflussanalyse (Business Impact Analysis)
12. Geschäftskontinuität (Business Continuity)
13. Sicherheit und Sicherheitsdreiklang
14. Risiko und Risikodreiklang
15. Risikomanagement
16. Zusammenfassung

4.1 Unternehmenssicherheitsmanagementsystem

Ein Unternehmenssicherheitsmanagementsystem (USMS), englisch Enterprise Safety, Security and Continuity Management System (ESSCMS), dient dazu, die Einhaltung des Sicherheits- und Kontinuitätsniveaus eines Unternehmens anforderungsgerecht und kontinuierlich sicherzustellen. Um dies zu realisieren, müssen geeignete Prozesse, Verantwortlichkeiten, Verfahren, Methodiken, Ressourcen und Hilfsmittel sowie eine angemessene Aufbauorganisation festgelegt und nachweisbar umgesetzt sein. Dies erfordert eine durchgängige, strukturierte, ganzheitliche, transparente, anschauliche und in der Praxis erprobte sowie dokumentierte Methodik zur anforderungsgerechten, effizienten, überwachten, gesteuerten und kontinuierlichen Absicherung eines Unternehmens, unter angemessener Berücksichtigung interner und externer Vorgaben und Anforderungen, beispielsweise gesetzliche, regulatorische, normative und vertragliche.

Ein USMS umfasst den durchgängigen Top-down-Aufbau, die Prozess- und Strukturorganisation, die Implementierung, die Schulung, den Betrieb, das durch Kontrollelemente und Kennzahlen sowie die Balanced Scorecard gestützte Monitoring, Controlling und Reporting sowie die Sensibilisierung, die Übung, die Prüfung, die Pflege und die Verbesserung sowie die Dokumentation. Es integriert das Sicherheits-, Kontinuitäts- und Risikomanagement sowie das Konformitätsmanagement.

Ein USMS enthält einen Sicherheits-, Kontinuitäts- und Risikomanagementprozess. Es verfügt zum einen über ein standardisierendes Rahmenwerk und über Dokumentationen (Vorgabedokumente) sowie zum anderen über Aufzeichnungen aus dem operativen Betrieb, z. B. sicherheitsrelevante Protokolle und Berichte.

Das USMS beinhaltet Kern-, Unterstützungs- und Begleitprozesse.

Ein USMS berücksichtigt den Lebenszyklus von Prozessen, Ressourcen, Produkten und Leistungen. So ermöglicht es die Realisierung von prozess- und lebenszyklusimmanenter sowie produkt- und leistungsimmanenter (service-immanenter) Sicherheit und Kontinuität.

Nach Kenntnis des Autors integriert derzeit nur die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller, wie sie im „Handbuch Unternehmenssicherheit“ des Autors beschrieben ist, diese Anforderungen an ein USMS.

4.2 Informationssicherheitsmanagementsystem

Ein Informationssicherheitsmanagementsystem (ISMS) dient dazu, die Einhaltung des Sicherheits- und Kontinuitätsniveaus von Informationen anforderungsgerecht und kontinuierlich sicherzustellen. Um dies zu realisieren müssen geeignete Prozesse, Verantwortlichkeiten, Verfahren, Methodiken, Ressourcen und Hilfsmittel sowie eine angemessene Aufbauorganisation festgelegt und nachweisbar umgesetzt sein. Dies erfordert eine durchgängige, strukturierte, ganzheitliche, transparente, anschauliche und in der Praxis erprobte sowie dokumentierte Methodik zur anforderungsgerechten, effizienten, überwachten, gesteuerten und kontinuierlichen Absicherung des Informationsmanagements einer Organisation, z. B. eines Unternehmens, unter angemessener Berücksichtigung interner und externer Vorgaben und Anforderungen, beispielsweise gesetzliche, regulatorische, normative und vertragliche.

Ein ISMS umfasst den durchgängigen Top-down-Aufbau, die Prozess- und Strukturorganisation, die Implementierung, die Schulung, den Betrieb, das durch Kontrollelemente und Kennzahlen sowie die Balanced Scorecard gestützte Monitoring, Controlling und Reporting sowie die Sensibilisierung, die Übung, die Prüfung, die Pflege und die Verbesserung sowie die Dokumentation. Es integriert das Sicherheits-, Kontinuitäts- und Risikomanagement sowie das Konformitätsmanagement.

Ein ISMS enthält einen Sicherheits-, Kontinuitäts- und Risikomanagementprozess. Es verfügt zum einen über ein standardisierendes Rahmenwerk und über Dokumentationen (Vorgabedokumente) sowie zum anderen über Aufzeichnungen aus dem operativen Betrieb, z. B. sicherheitsrelevante Protokolle und Berichte.

Das ISMS beinhaltet Kern-, Unterstützungs- und Begleitprozesse.

Ein ISMS berücksichtigt den Lebenszyklus von Prozessen, Ressourcen, Produkten und Leistungen. So ermöglicht es die Realisierung von prozess- und lebenszyklusimmanenter sowie produkt- und leistungsimmanenter (service-immanenter) Sicherheit und Kontinuität.

Nach Kenntnis des Autors integriert derzeit nur die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller, wie sie in „IT-Sicherheit mit System“ des Autors beschrieben ist, diese Anforderungen an ein ISMS. Verschiedene Teilbereiche bzw. Kernelemente eines ISMS finden sich in unterschiedlicher Ausprägung, Vollständigkeit, Detaillierung, Konkretisierung und Qualität sowie teilweise nach Erscheinen von Büchern oder Artikeln des Autors in bestehenden Standards und

Practices, z. B. in der im Aufbau befindlichen Normenreihe ISO/IEC 27000 sowie der ISO 17799:2005 und der ISO/IEC 13335 sowie im IT-Grundschutzhandbuch des BSI und im ITIL® Security Management.

4.3 Sicherheitsmanagement

Unter Sicherheitsmanagement wird im Folgenden der Prozess zum Aufbau, zum Betrieb sowie zur kontinuierlichen Prüfung, Steuerung und Fortentwicklung des Sicherheitsniveaus eines Unternehmens verstanden.

Schutzobjekte

Sicherheitsmanagement als Ganzes bezieht sich auf das Gesamtunternehmen mit all seinen personellen, materiellen und immateriellen Werten. Zu den materiellen Werten gehören u. a. Gebäude mit ihren Räumen und der haustechnischen Infrastruktur, Fertigungsstraßen, Produktionsanlagen, Maschinen, Informations- und Kommunikationssysteme, Arbeitsmittel, Materialien und finanzielle Mittel. Demgegenüber stellen Daten, Image und Know-how immaterielle Werte dar.

Diese Werte (assets) sind gleichzeitig Schutzobjekte, die es anforderungsgerecht abzusichern gilt. Sicherheitsmanagement erstreckt sich vom Objektschutz über sichere Geschäftsprozesse bis hin zum Schutz von Arbeitsmitteln und IT-Systemen sowie von der Arbeitssicherheit bis hin zum Personenschutz.

Prozesse, Ressourcen und Organisation

Sicherheitsmanagement umfasst die Themenfelder Prozesse, Ressourcen (von Technik über Methoden bis Personal) und Organisation. Die Erfahrung zeigt mir, dass das Zusammenspiel dieser Aspekte ein entscheidender Erfolgsfaktor beim Aufbau und der Weiterentwicklung des Sicherheitsmanagements ist.

Lebenszyklus

Ein weiterer Aspekt des Sicherheitsmanagements ist der Lebenszyklus von Prozessen, Ressourcen (Systemen), Dienstleistungen und Produkten. Um einen sicheren Geschäftsbetrieb, sichere Systeme und sichere Produkte zu erreichen, müssen Sicherheitsaspekte frühzeitig berücksichtigt werden. Der Lebenszyklus beginnt beispielsweise mit einer Idee, der sich eine Machbarkeitsstudie und eine Konzeption anschließen. In diesen Phasen sind ebenso wie bei der späteren Entwicklung, dem Betrieb und schließlich der Außerbetriebnahme Sicherheitsaspekte zu berücksichtigen.

Integrative Teilbereiche des Sicherheitsmanagements sind z. B. das Sicherheitsmanagement der Geschäftsprozesse oder der Informations- und Telekommunikationstechnologie (ITK). Sicherheit der ITK erstreckt sich über alle Komponenten, wie z. B. Hard- und Software,

Dataware, Processware (Prozesse), Knowledgeware (Wissen) und Paperware (Unterlagen und Dokumente).

4.4 ITK-Sicherheitsmanagement

ITK-Sicherheitsmanagement beinhaltet den Aufbau, die kontinuierliche Prüfung, Steuerung und Fortentwicklung der Sicherheit in den Bereichen der Informations- und Telekommunikationstechnik (ITK). Im Bereich der Informationstechnik erstreckt es sich über alle IT-Prozesse, die Phasen des Lebenszyklus von Computersystemen sowie über alle Komponenten, wie z. B. Hardware, Software und Dokumentation.

Insbesondere in den letzten Jahren sind im IT-Bereich Normen und Standards sowie Good und Best Practices entstanden oder haben sich deutlich weiter entwickelt. Hierzu gehören Normen wie die ISO 13335, die ISO 17799, die ISO 27001, aber auch Best Practices à la ITIL®, die Maßnahmen der BSI-IT-Grundschutzkataloge, die Information Security Governance des IT Governance Institute® und die Control Objectives for Information and related Technology (COBIT®), die sich teils überlappen und teils unterschiedliche Ansätze verfolgen.

Normen

Nicht zuletzt zu nennen ist hier die vom Autor veröffentlichte dreidimensionale Sicherheitspyramide [4], die Interesse und positive Resonanz in Wirtschaft und Lehre gefunden hat. Deren erste Dimension bezieht sich auf die durchgängige hierarchische Struktur, die zweite Dimension auf Prozesse, Ressourcen und Personal sowie Organisation und die dritte Dimension auf den Lebenszyklus. In der Hierarchieebene Richtlinien wurden im Buch „IT-Sicherheit mit System“ [4] im Jahr 2003 u. a. beispielhafte Richtlinien angegeben. Sie beziehen sich auf die E-Mail-Nutzung, den Virenschutz, die Datensicherung und die Notfall- und Katastrophenvorsorge.

Sicherheitspyramide

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Jahr später, im Juni 2004 ebenfalls verschiedene Beispielskonzepte bzw. Sicherheitsrichtlinien für wichtige Sicherheitsthemen veröffentlicht. Diese beziehen sich u. a. auch auf die E-Mail-Nutzung, den Computer-Viren-Schutz, die Datensicherung und die Notfallvorsorge und dürften sich in der Praxis als ähnlich hilfreiche Basis erweisen, wie die des Autors.

Beispielskonzepte des BSI und Parallelen zur Sicherheitspyramide

Ähnlich wie Ende Juli 2003 vom Autor in „IT-Sicherheit mit System“ [4] veröffentlicht, hat es sich laut dem später veröffentlichten und im Internet zum Zeitpunkt der Einsichtnahme datumsfreien BSI-Dokument „Zielgruppengerechte Vermittlung von IT-Sicherheits-

themen“ bewährt, einen hierarchischen Aufbau von Richtlinien zu wählen. Dieser beginnt bei der Sicherheitsleitlinie mit Sicherheitszielen und –strategie. In der nächsten Ebene finden sich Richtlinien, z. B. zur Internetnutzung oder zum Virenschutz, die – wie auch bei der Sicherheitspyramide – nicht auf konkrete Produkte eingehen, um – wie es dort heißt „zunächst die grundlegenden Voraussetzungen zu erarbeiten und Vorgaben zu kennen“. Die dritte und unterste Ebene bilden die konkreten Maßnahmen, technischen Details und produktspezifischen Einstellungen.

Diese drei Ebenen sind dort – ähnlich der hierarchischen Dimension der Sicherheitspyramide des Autors – dreiecksförmig und hierarchisch dargestellt. Sie bestätigen nach Auffassung des Autors durch ihre deutlichen prinzipiellen Analogien zu den Ebenen Sicherheitspolitik, -ziele, -richtlinien, -konzepte und -maßnahmen der dreidimensionalen Sicherheitspyramide des Autors dessen Vorgehensmodell. Letzteres enthält allerdings noch viele weitergehende Aspekte und wurde bereits Mitte der 90er Jahre des vorigen Jahrhunderts in komprimierter Form veröffentlicht [5]. In den IT-Grundschrutskatalogen vom November 2006 befindet sich erstmals die Abbildung eines dreistufigen hierarchischen Aufbaus im Kapitel M 2.338, die im IT-Grundschrutskatalog 2005 noch nicht vorhanden war, sowie die dazugehörige Beschreibung.

*Internationale
Standardisie-
rung
wünschenswert*

In diesem Kontext erscheint es mir empfehlenswert, wenn die historisch entstandene Vielfalt in Form teils branchenübergreifender teils branchenspezifischer nationaler und internationaler Normen, (de-facto-) Standards und Good bzw. Best Practices in Zukunft zu einer internationalen Norm zusammengeführt würden. Ziel müsste es sein, eine konsistente, ganzheitliche, durchgängige, systematische und anschauliche Vorgehensweise für das Informationssicherheitsmanagement zu entwickeln, ähnlich wie sie die dreidimensionale Sicherheitspyramide des Autors bietet.

Die folgenden Unterkapitel erläutern die Elemente verschiedener Normen und Practices und zeigen, wo diese Ansätze in der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller bereits berücksichtigt sind. Eine überblicksartige Darstellung des Autors zu diesem Thema findet sich in [8].

4.4.1 ISO/IEC 13335-1:2004

Die ISO 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 2004, bildet den ersten Teil

der Normenreihe ISO 13335. Sie ersetzt die vorherigen Versionen in Form der ISO/IEC TR 13335-1:1996 und der ISO/IEC TR 13335-2:1997. Thematisch beschäftigt sich die ISO 13335-1:2004 mit der Sicherheit von Informations- und Kommunikationstechnologie. Sie weitet damit das Blickfeld von der IT-Sicherheit aus auf die Sicherheit der Kommunikationstechnologie. Dementsprechend verwendet sie den Begriff ICT, also das englische Akronym für Informations- und Kommunikationstechnologie (IKT bzw. IuK) bzw. Informations- und Telekommunikationstechnologie (ITK). Die Norm betrachtet die Planung, die Implementierung und den Betrieb einschließlich der Wartung. Die Inhalte bewegen sich auf überblicksartigem Management-Niveau.

Kapitel 2 des Standards stellt 26 übergreifende Definitionen sicherheitsrelevanter Begriffe bereit. Kapitel 3 erläutert überblicksartig wesentliche Sicherheitskonzepte und den Zusammenhang zwischen verschiedenen Sicherheitselementen. Das Kapitel geht ein auf Sicherheitsprinzipien, Werte, Bedrohungen, Verwundbarkeiten, Auswirkungen, Risiken, Sicherheitsmaßnahmen und Rahmenbedingungen.

Kapitel 4 geht ein auf Sicherheitsziele, -strategien und die vier hierarchischen Ebenen der Sicherheitspolitik. Ausgangspunkt ist die unternehmensweite Sicherheitspolitik. Aus ihr leitet sich in der nächsten Ebene die Informationssicherheitspolitik ab, gefolgt von der unternehmensweiten ITK-Sicherheitspolitik und schließlich der Sicherheitspolitik des jeweiligen ITK-Systems.

Das Kapitel 5 beschreibt die Rollen und Verantwortlichkeiten sowie die Organisationsstruktur für effektive ITK-Sicherheit. Die sicherheitsrelevanten Rollen folgen – wie zuvor die Sicherheitspolitik – einem hierarchischen Ansatz. Dementsprechend sieht der Standard Security Officers auf Unternehmensebene einerseits für das Unternehmen und andererseits für die ITK vor. Weitere ITK-Sicherheitsbeauftragte (ICT Security Officer) befinden sich auf Bereichs-, Projekt- und Systemebene. Den Abschluss bildet der ITK-Sicherheitsadministrator.

Als Gremien identifiziert die ISO den ITK-Lenkungsausschuss (ICT Steering Committee) und das ITK-Sicherheitsforum (ICT Security Forum). Gegenüber dem vorherigen Technical Report in Form der ISO/IEC TR 13335-1 führt die Normfassung von 2004 überblicksartig einen vierstufigen ITK-System-Lebenszyklus an. Im Unterkapitel organisatorische Prinzipien weist sie darauf hin, dass ITK-Sicherheit in alle Phasen des ITK-System-Lebenszyklus integriert sein sollte. Der hier vierstufige ICT-System-Lebenszyklus weist Parallelen zum drei-

stufigen IT-System-Lebenszyklus des Technical Reports ISO/IEC TR 13335-2:1997 auf.

Kapitel 6 schließlich gibt einen ersten Überblick über die ITK-Sicherheitsmanagementfunktionen bei Planung und Implementierung sowie bei Betrieb und Wartung.

*ISO/IEC
13335-2* Die ISO/IEC 13335-2 Information technology – Security techniques – Management of information and communications technology security – Part 2: Techniques for information and communications technology security risk management befindet sich laut Vorwort zur ISO 13335-1:2004 in Vorbereitung. Diese ISO-Norm soll die früheren Technical Reports ISO/IEC TR 13335-3:1998, Techniques for the management of Information Technology security, und ISO/IEC TR 13335-4:2000, Selection of safeguards, aufnehmen.

*ISO/IEC
13335-5:2001* Die ISO/IEC 13335-5:2001 schließlich, die sich mit Netzsicherheit befasst, befindet sich in Überarbeitung. Sie soll mit der ISO/IEC 18028-1, Information technology – Security techniques – IT network security – Part 1: Network security management zusammengeführt und durch diese ersetzt werden.

*Vergleich zur
Sicherheits-
pyramide* Die ISO 13335-1:2004 besitzt einen tendenziell hierarchischen Aufbau, der von der unternehmensweiten Sicherheitspolitik ausgeht. Die dreidimensionale Sicherheitspyramide bietet ein darüber hinausgehendes hierarchisches Modell, das ebenfalls von der Sicherheitspolitik auf Unternehmensebene ausgeht und hierbei Kontinuitäts- und Risikomanagement berücksichtigt. Die unternehmensweite ITK-Sicherheitspolitik der ISO erscheint vergleichbar mit der Ebene der Richtlinien und die Sicherheitspolitik des ITK-Systems mit der Ebene der Konzepte in der Sicherheitspyramide nach Dr.-Ing. Müller. Die Sicherheitspyramide stellt zusätzlich die systematische Überführung von Ebene zu Ebene bereit. Weiterhin behandelt die Sicherheitspyramide seit jeher umfangreich Prozessthematiken und einen deutlich detaillierteren Lebenszyklus ([5], [6], [7]).

4.4.2 ISO/IEC 17799:2005, ISO/IEC 27002:2005

*ISO/IEC
17799:2005* Die ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management ist eine Überarbeitung der ISO/IEC 17799:2000, die aus dem British Standard BS 7799-1:2000 hervorging. Seit Juli 2007 heißt sie ISO/IEC 27002:2005. Sie behandelt u. a. die folgenden zwölf Themenfelder und Themen:

*ISO/IEC
27002:2005*

1. Risikobewertung und –behandlung
(Risk Assessment and Treatment)
Bewertung und Behandlung von Risiken
2. Sicherheitspolitik/Sicherheitsleitlinie
(Security Policy)
Erstellung, Prüfung und Bekanntgabe einer schriftlichen Sicherheitspolitik sowie deren Review
3. Organisation der Informationssicherheit
(Organization of Information Security)
Interne Organisation sowie Dritte
4. Management der Unternehmenswerte
(Asset Management)
Verantwortlichkeiten für das Inventar und Klassifizierung desselben
5. Personalsicherheit
(Human Resources Security)
Verantwortlichkeiten und Sicherheitsaspekte vor und während des Beschäftigungsverhältnisses sowie bei Beendigung desselben oder bei Veränderungen, u. a. im Hinblick auf die Rückgabe ausgehändigter Wertobjekte und die Anpassung bzw. Löschung von Zugangs- und Zugriffsrechten
6. Physische und Umgebungssicherheit
(Physical and Environmental Security)
Sicherheitszonen, Umgebungssicherheit, Zutrittskontrolle, Absicherung von Räumlichkeiten und Schutz vor externen Bedrohungen sowie Gerätesicherheit
7. Management von Kommunikation und Betrieb
(Communications and Operations Management)
Organisation mit Change Management und Funktionstrennung sowie Trennung von Entwicklung, Test und Produktion, Management externer Dienstleistungen, Systemplanung und –abnahme, Schutz vor böartigem Code, Backup, Netzsicherheit, Umgang mit Datenträgern, Informationsaustausch, Monitoring
8. Zugangskontrolle
(Access Control)
Zugangs- und Zugriffsschutz, Passwortgebrauch, clear desk and clear screen policy, Netzzugang und Netzsegmentierung, Zugang zum Betriebssystem, zu Anwendungen und zu Informationen, mobile computing und Telearbeit,
9. Beschaffung, Entwicklung und Wartung von Informationssystemen
(Information Systems Acquisition, Development and Maintenance)
Anforderungsanalyse und Anforderungsspezifikation, Kontrolle

von Input, Verarbeitung und Output, Schutz durch Verschlüsselung, Schutz der Systemdateien und des Quellcodes, Sicherheit im Entwicklungs- und Supportprozess

10. Management informationssicherheitsrelevanter Ereignisse
(Information Security Incident Management)

Berichte zu sicherheitsrelevanten Ereignissen und entdeckten Sicherheitsdefiziten, Verantwortlichkeiten und Verfahren zum Umgang mit verschiedenen sicherheitsrelevanten Ereignissen einschließlich Beweissicherung und Notfallplanung, quantitative Bewertung und Monitoring sicherheitsrelevanter Ereignisse im Hinblick auf Art, Anzahl und verursachte Kosten

11. Management der Geschäftskontinuität
(Business Continuity Management)

Unternehmensweite Etablierung und Pflege des Business Continuity Managements unter Berücksichtigung der Informationssicherheit, Risikoinventur mit Bedrohung, Eintrittswahrscheinlichkeit und Auswirkungen, Entwicklung eines durchgängigen und in sich konsistenten Rahmenwerks zum Business Continuity Management, Entwicklung, Einführung, Test und Pflege der Pläne zum Erhalt der Geschäftskontinuität

12. Konformität
(Compliance)

Identifikation aller relevanten gesetzlichen, aufsichtsbehördlichen und vertraglichen Verpflichtungen, Berücksichtigung des Urheberrechts, gesetz-, aufsichts- und vertragskonformer Schutz von Informationen gegen Verlust, Zerstörung oder Verfälschung

*Vergleich zur
Sicherheits-
pyramide*

Die dreidimensionale Sicherheitspyramide enthält Themenstellungen, die auch die ISO 17799:2005 bzw. ISO 27002:2005 anspricht, und stellt darüber hinaus Zusammenhänge her. Sie ergänzt, systematisiert und veranschaulicht die unterschiedlichen Themen. Beispiele hierfür sind die Sicherheitspyramide selbst sowie das Sicherheitsschalenmodell nach Dr.-Ing. Müller.

4.4.3 ISO/IEC 27001:2005

*ISO/IEC
27001:2005*

Die ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, behandelt auf sehr überblicksartiger Ebene die Themen

1. Begriffe und Definitionen
2. Informationssicherheitsmanagementsysteme (ISMS)
3. Verantwortung des Managements
4. Internes ISMS Audit

5. Management Review des ISMS
6. Verbesserung des ISMS
7. Kontrollziele und Kontrollen (Anhang A)
8. OECD-Prinzipien und der Standard ISO/IEC 27001:2005 (Anhang B).

Bei der Beschreibung des ISMS folgt die ISO/IEC 27001:2005 einem prozessorientierten Ansatz. Er basiert auf dem PDCA-Zyklus (Plan-Do-Check-Act), der aus dem Qualitätsmanagement bekannt ist. Die Planungsphase (Plan) beschreibt den Aufbau des ISMS. Die folgende Durchführungsphase (Do) widmet sich der Implementierung und dem Betrieb. Die Prüfungsphase (Check) soll durch Monitoring und Reviews frühzeitig Sicherheitsdefizite und Verbesserungspotenziale aufzeigen. Die Verbesserungsphase (Act) schließlich hat ihren Fokus auf der Wartung, Korrektur und Verbesserung.

*PDCA-Zyklus
für das ISMS*

In der Planungsphase legt die Organisation, z. B. ein Unternehmen oder eine Behörde, den Geltungsbereich und Rahmen für das ISMS fest. Sie orientiert sich an den Sicherheitsanforderungen und -erwartungen der interessierten Parteien. (Anmerkung des Autors: Die Sicherheitspyramide nach Dr.-Ing. Müller, die ebenfalls den PDCA-Zyklus für den Sicherheitsmanagementprozess nutzt, fasst Anforderungen und Erwartungen als explizite und implizite Anforderungen der Bezugsgruppen zusammen.) Sie berücksichtigt jene gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen, die für sie relevant sind. Danach führt sie eine Risikoinventur durch, d. h. sie erhebt, analysiert und bewertet ihre Risiken. Zur Optimierung ihres Risikoportfolios identifiziert sie Handlungsoptionen und bewertet diese.

Die Durchführungsphase konzentriert sich auf die Implementierung des Risikomanagements und geeigneter Kontrollen sowie den Betrieb des ISMS. Schulungsprogramme spielen eine wesentliche Rolle.

Die Prüfungsphase beinhaltet die Überwachung und Prüfung des ISMS. Das Monitoring unterstützt bei der frühzeitigen Entdeckung von Fehlern und sicherheitsrelevanten Ereignissen. Regelmäßige Reviews und Audits prüfen das ISMS und identifizieren Verbesserungspotenziale.

In der Verbesserungsphase setzt die Organisation die entdeckten Optimierungsmöglichkeiten im ISMS um. Sie kommuniziert die vorgenommenen Änderungen und stellt sicher, dass sie das gewünschte Ziel erreichen.

Zur Steuerung des ISMS gibt die ISO/IEC 27001:2005 im Anhang A Kontrollziele und Kontrollen an. Diese sind abgeleitet aus den

*Kontrollziele
und Kontrollen*

Themen, die die ISO/IEC 17799:2005 behandelt und beziehen sich dementsprechend auf folgende Bereiche:

1. Sicherheitspolitik
2. Organisation der Informationssicherheit intern und gegenüber Dritten
3. Management der Unternehmenswerte
4. Personelle Sicherheit
5. Physische und Umgebungssicherheit
6. Management von Kommunikation und Betrieb
7. Zugangs- und Zugriffskontrolle
8. Beschaffung, Entwicklung und Wartung von Informationssystemen
9. Management informationssicherheitsrelevanter Ereignisse
10. Management der Geschäftskontinuität
11. Konformität (Compliance)

*Vergleich zur
Sicherheits-
pyramide*

Die ISO 27001:2005 beschreibt auf sehr überblicksartiger Ebene den Sicherheitsmanagementprozess und seine Inhalte. Sie baut auf dem PDCA-Zyklus auf. Die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller enthält den Sicherheitsmanagementprozess, der sich ebenfalls am PDCA-Zyklus orientiert. Die Norm führt im Anhang Kontrollziele und Kontrollen an. Die dreidimensionale Sicherheitspyramide verfügt durch das Reifegradmodell, die Hierarchieebenen und Prozesse sowie den Sicherheitsregelkreis über Kontrollen und Kennzahlen.

4.4.4 ISO/IEC 27000-Reihe

Das ISM ist zentrales Thema der geplanten ISO 27000-Reihe. Über die ISO 27001:2005 hinaus sind derzeit verschiedene weitere Standards zur IT-Sicherheit angedacht, in Entwicklung oder veröffentlicht. Die ISO 17799:2005 ist seit Juli 2007 in ISO 27002:2005 umbenannt. Implementierungsrichtlinien sollen sich in der ISO 27003 finden und Metriken sowie Messmöglichkeiten in der ISO 27004. Für das Risikomanagement ist die ISO 27005 vorgesehen. Die ISO 27006:2007 spezifiziert Anforderungen an Auditierungs- und Zertifizierungsinstanzen von ISMS. Der Standard unterstützt in erster Linie die Akkreditierung von ISMS-Zertifizierern. Er enthält zusätzlich Hinweise zur Interpretation dieser Anforderungen. Die folgende Abbildung gibt einen Überblick über die Planungen und Überlegungen der ISO. Sie stützt sich ebenso wie die vorangegangenen Ausführungen

auf die in der Abbildung angegebenen Quellen sowie die bereits vorhandenen Normen.

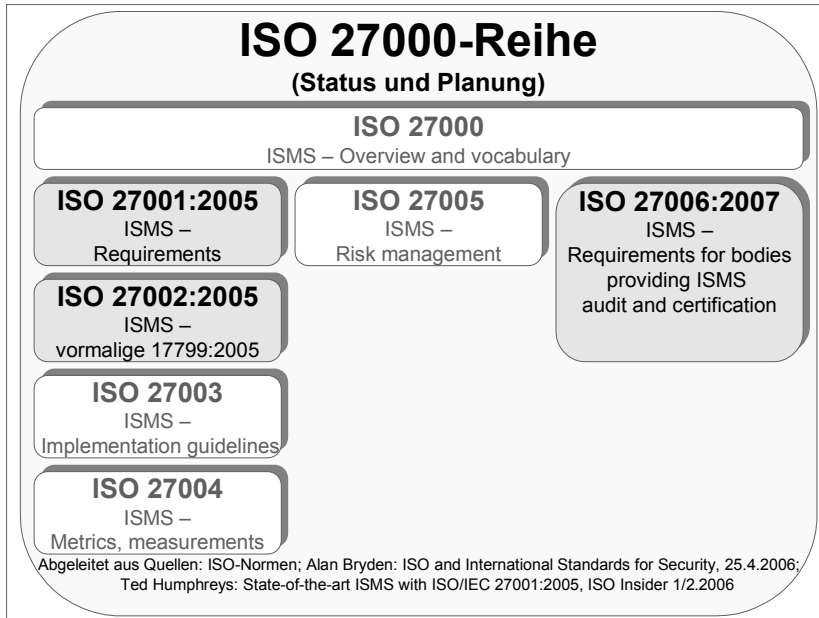


Abb. 4.1: ISO 27000-Reihe

4.4.5 ITIL® Security Management

Die Version 2 von ITIL®, der IT Infrastructure Library des Office of Government Commerce (OGC) stellt den dortigen Ausführungen zufolge einen Satz von Best Practices bereit, die auf der kollektiven Erfahrung kommerzieller und öffentlicher Praktiker weltweit basieren. Laut ITIL® hat sich die ITIL®-Vorgehensweise zu einem De-facto-Standard entwickelt, den einige der weltweit führenden Unternehmen einsetzen. Umfragen zufolge besitzt die ITIL®-orientierte Vorgehensweise auch in Deutschland einen hohen Verbreitungsgrad.

Das ITIL®-Buch „Best Practice for Security Management“ (8. Auflage 2004, Erstveröffentlichung 1999) ist überblickartig geschrieben. Es untergliedert sich in die Grundlagen der IT-Sicherheit, den Zusammenhang zwischen Security Management und ITIL®-Prozessen, Maßnahmen zum Security Management sowie Richtlinien zum Aufbau des Security Managements. Der dortige Anhang A stellt in Form einer Tabelle den Bezug zum British Standard BS 7799-1 her, aus dem die ISO 17799:2005 hervorgegangen ist. In der Tabelle sind den Kapiteln bzw. Unterkapiteln des BS 7799-1 die entsprechenden Kapitel im

*ITIL® Security
Management*

ITIL®-Buch zum Security Management gegenübergestellt bzw. zusammenfassende Beschreibungen dazu.

Das ITIL® Security Management hat Auswirkungen auf die ITIL®-Prozesse des Servicemanagements. Diese fasst ITIL® in den Themenkomplexen Service Support und Service Delivery zusammen. Service Support beinhaltet die operativen Prozesse Incident Management mit der Funktion des Service Desk sowie Problem -, Change -, Configuration - und Release Management. Service Delivery enthält die taktischen Prozesse Service Level -, Performance - und Capacity -, Availability - und Business Continuity - sowie Financial Management.

Sicherheitsmanagement-Prozess

Der Sicherheitsmanagementprozess nach ITIL® besteht aus den Phasen Plan, Implement, Evaluate und Maintain, die dem PDCA-Zyklus ähneln. Die Planung beinhaltet hierbei die Politik sowie Service Level Agreements (SLA) und Underpinning Contracts (UC). Die Implementierungsphase behandelt u. a. die Klassifizierung, die personelle und physische Sicherheit sowie das Management von Zugangsrechten. Die Evaluierungsphase beinhaltet interne und externe Audits.

Viel „was“, weniger „wie“

Die Best Practices nach ITIL® legen ihren Schwerpunkt in der Version 2 auf das Servicemanagement. Sie beschreiben dort vorrangig, was zu tun ist, und weniger, wie dies zu tun ist. Das Servicemanagement mit den Büchern zum Service Support und Service Delivery ist recht weit entwickelt. Demgegenüber stellt sich das ITIL® Security Management sehr überblicksartig dar.

Vergleich zur Sicherheitspyramide

Gegenüber ITIL® besitzt die dreidimensionale Sicherheitspyramide des Autors einerseits ähnliche und andererseits zusätzliche Managementdisziplinen bzw. Begleitprozesse. Sie differenziert ferner zwischen den Prozessarten Kern-, Unterstützungs- und Begleitprozess. Außerdem verfügt sie über die Sicherheitshierarchie sowie eine weiter gefasste Lebenszyklusbetrachtung. Durch konkrete Beispiele veranschaulicht dieses Buch verschiedentlich das „wie“ der Umsetzung.

4.4.6 IT-Grundschutzhandbuch, IT-Grundschutzkataloge des BSI

IT-Grundschutzhandbuch und IT-Grundschutzkataloge

Das IT-Grundschutzhandbuch (IT-GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat Ende 2005 eine neue Struktur erhalten: Es besteht nun aus zwei Teilen, der Grundschutz-Vorgehensweise und den IT-Grundschutzkatalogen (IT-GSK), die sich aus Gefährdungs- und Maßnahmenkatalogen zusammensetzen. Der Umfang der IT-Grundschutzkataloge zusammen mit der bisher jährlichen Aktualisierung stellt aus meiner Sicht eine Stärke des IT-Grundschutzhandbuchs dar, verglichen mit den eher übergreifend orientierten internationalen Standards und Normen.

Der geeignete Einsatz des IT-Grundschutzes nach BSI soll – wie der BSI-Standard 100-2, Version 1.0, Dezember 2005 ausführt – ein IT-Sicherheitsniveau ermöglichen, das einem „normalen“ Schutzbedarf und dem Stand der Technik entspricht. Das IT-GSHB:2005 einschließlich der BSI-Standards beschreibt den IT-Sicherheitsprozess sowie eine Vorgehensweise für den Aufbau des IT-Sicherheitsmanagements. Die IT-Grundschutzkataloge als Teil des IT-Grundschutzes enthalten umfangreiche Gefährdungs- und Maßnahmenkataloge.

Der IT-Sicherheitsprozess nach BSI besteht aus den folgenden drei Kernaktivitäten:

1. IT-Sicherheitsprozess initiieren
2. IT-Sicherheitskonzeption erstellen
3. IT-Sicherheit aufrechterhalten und verbessern

In der Initiierungsphase äußert sich die Leitungsebene zu ihrer Verantwortung. Außerdem legt sie fest, wie der IT-Sicherheitsprozess zu planen und zu konzipieren ist. Die Initiierungsphase umfasst darüber hinaus den Aufbau der Organisation und die Erstellung der Leitlinie sowie die Bereitstellung der Ressourcen für die IT-Sicherheit.

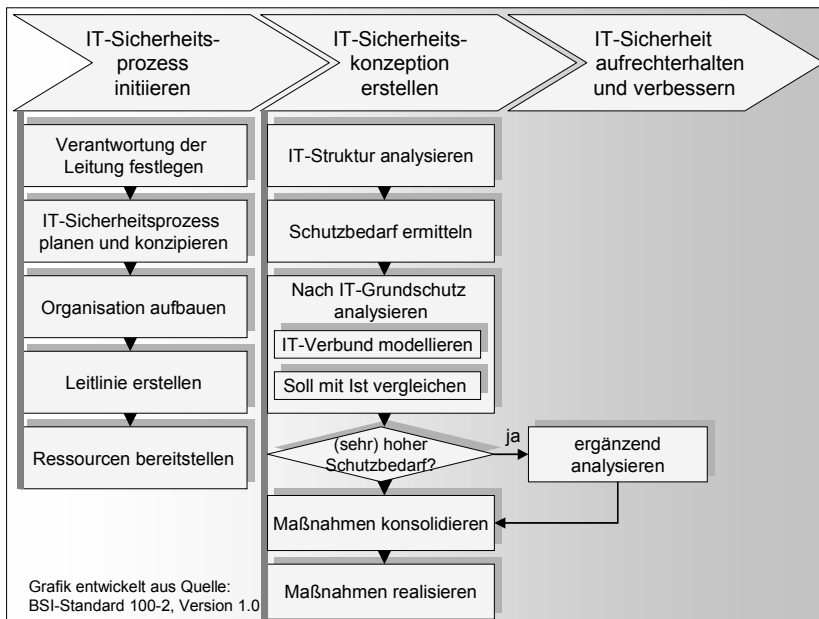


Abb. 4.2: IT-Sicherheitsprozess orientiert an BSI

Um im nächsten Schritt die IT-Sicherheitskonzeption zu erstellen, sind die folgenden Aktivitäten vorgesehen:

1. IT-Struktur analysieren, bestehend aus Systemen und Anwendungen sowie deren Abhängigkeiten bis hin zu den Rahmenbedingungen organisatorischer und personeller Art
2. Schutzbedarf ermitteln für Anwendungen und IT-Systeme
3. Nach IT-Grundschutz analysieren und die erforderlichen Grundschutzmaßnahmen modellieren sowie im Rahmen des Basis-Sicherheitschecks einen Soll-Ist-Vergleich durchführen
4. Ergänzende Sicherheitsanalyse durchführen, wenn ein hoher oder sehr hoher Schutzbedarf vorliegt
5. Maßnahmen konsolidieren
6. Maßnahmen realisieren

Schichtenmodell

Die IT-Grundschutzkataloge bestehen seit dem IT-GSHB 2005 aus Bausteinkatalogen, die in fünf Schichten unterteilt ist. Diese Schichten fassen einzelne Bausteine zu einer Gruppe zusammen. Bis auf die Schicht 1, die übergreifende Aspekte betrachtet, handelt es sich bei den Schichten um Ressourcengruppe, und zwar für Infrastruktur, IT-Systeme, Netze und IT-Anwendungen. Die Schichten im Einzelnen:

1. Übergeordnete IT-Sicherheitsaspekte
Hierunter sind IT-Sicherheitsthemen zu verstehen, die für das IT-Sicherheitsmanagement als Ganzes oder für mehrere IT-Komponenten gelten. Sie erstrecken sich vom IT-Sicherheitsmanagement, über Organisation, Personal, Notfallvorsorge, Datensicherung und Datenschutz, bis schließlich hin zu Archivierung und Schulung.
2. Infrastrukturelle Sicherheit
Diese Schicht bietet Bausteine für die bauliche und infrastrukturelle Sicherheit, z. B. für Gebäude, Arbeitsplätze, Serverraum, Rechenzentrum, Datensicherungsarchiv und Räume für technische Infrastruktur.
3. Sicherheit der IT-Systeme
Diese Schicht enthält Bausteine für Clients, z. B. unter UNIX® oder Windows®, für Server, z. B. unter UNIX®, Windows® oder Novell®, für zSeries®-Mainframes sowie für Netzkomponenten, wie Sicherheit gateways, Router und Switches, aber auch für TK-Anlagen, Faxgeräte; Anrufbeantworter, Mobiltelefone und PDAs.
Anmerkung des Autors: Diese Schicht müsste aufgrund der dort behandelten Kommunikationssystemen nach Auffassung des Autors

und unter Berücksichtigung der Begriffswahl der ISO/IEC 13335 eigentlich ITK-Systeme heißen.

4. Netzsicherheit

In diese Schicht fallen Bausteine für heterogene Netze, Netz- und Systemmanagement, LAN-Anbindung, WLAN, VoIP und remote Access.

5. Sicherheit in Anwendungen

Diese Schicht beinhaltet u. a. Bausteine für den Datenträgeraustausch, für Webserver, Lotus Notes®, Workgroup- und E-Mail-Systeme, Datenbanken sowie SAP®-Systeme.

Im Vergleich mit der Sicherheitspyramide haben die ressourcenspezifischen Bausteine der IT-GSK ihre Entsprechung in einer der hierarchischen Ebenen der ressourcenspezifischen PROSim-Dimension der Sicherheitspyramide. Die Schicht 1, übergreifende Aspekte, der IT-GSK ist u. a. vergleichbar mit den Sicherheitsrichtlinien bzw. generischen Sicherheitskonzepten der Sicherheitspyramide.

*Vergleich mit
der Sicherheits-
pyramide nach
Dr.-Ing. Müller*

In den Bausteinen der IT-Grundschutzkataloge hat das BSI erstmals im Jahr 2005 das Thema „Lebenszyklus“ aufgenommen, das Lesern von „IT-Sicherheit mit System“ und vom „Handbuch Unternehmenssicherheit“ seit längerem bekannt ist. Das in den IT-Grundschutzkatalogen dargestellte Lebenszyklusmodell besteht aus folgenden Phasen:

Lebenszyklus

- „Planung und Konzeption“,
- „Beschaffung“,
- „Umsetzung“,
- „Betrieb“,
- „Aussonderung“ und
- „Notfallvorsorge“.

Das BSI-Lebenszyklusmodell weist Parallelen zum seit längerem bekannten Lebenszyklusmodell der Sicherheitspyramide auf, aber auch Unterschiede, indem es beispielsweise die Notfallvorsorge als eigene Phase des Lebenszyklus betrachtet.

*Parallelen zur
Sicherheits-
pyramide nach
Dr.-Ing. Müller*

Im IT-Grundschutzkatalog vom November 2006 taucht erstmals die Maßnahme M 2.378, „System-Entwicklung“, als eigenständiges Element auf. Angabegemäß orientiert sie sich am V-Modell sowie teilweise den Vorgaben der ITSEC/CC. Sie besteht aus den Phasen Anforderungsdefinition, Architektur- oder Fach-Entwurf, Fein-Entwurf und Realisierung sowie den dort zu erreichenden Phasenergebnissen.

Den Mindestanforderungen an die Entwicklungsumgebung mit Themen wie Namenskonventionen, Verwaltung von Zwischen- und Endergebnissen, Festschreibung von Entwicklungsergebnissen sowie kontrollierte Bearbeitung von Änderungen folgt die Qualitätssicherung. Anschließend widmet sich das Kapitel den Themen Überführung in die Produktion und Software-Wartung sowie Problemmanagement.

*Parallelen zur
Sicherheits-
pyramide nach
Dr.-Ing. Müller*

Leser von „IT-Sicherheit mit System“ und verschiedenen auch sehr frühen Veröffentlichungen des Autors (z. B. [1], [5], [6], [9]) kennen diese Thematik unter dem Begriff Lebenszyklus, angereichert um die Begleitprozesse, wie z. B. das Änderungs-, Konfigurations-, Problem- und Qualitätsmanagement, sowie u. a. um das Prinzip der Namenskonventionen und Sicherheitsanforderungen an die Entwicklungsumgebung. Der Lebenszyklus von IT-Systemen beginnt beim Autor jedoch früher, ist umfangreicher und endet später. Ausgangspunkt ist die Beantragung und Planung, der die Anforderungsspezifikation sowie das technische Grob- und Feinkonzept folgen. Über Entwicklung, Test, Freigabe und weitere Phasen erstreckt sich der Lebenszyklus auf die Inbetriebnahme, den Betrieb und die Außerbetriebnahme. Phasen enden mit Ergebnissen in Form von Ergebnistypen und Qualitätssicherungsmaßnahmen, dargestellt in der Phasen-Ergebnistypen-Tabelle des Autors.

*Standards des
BSI*

Die bereits erwähnten Standards der 100er Reihe des BSI umfassen drei Dokumente:

- Der BSI-Standard 100-1, Version 1.0 vom Dezember 2005 legt Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) fest. Basis dieses BSI-Standards ist die ISO 27001. In diesem Standard beschreibt das BSI u. a. den oben genannten BSI-spezifischen Lebenszyklus von Sicherheitsmaßnahmen sowie den in der ISO 27001 angegebenen PDCA-Zyklus des IT-Sicherheitsprozesses.
- Der BSI-Standard 100-2, Version 1.0 vom Dezember 2005, beschreibt die Vorgehensweise nach IT-Grundschutz.
- Der BSI-Standard 100-3, Version 2.0, vom Dezember 2005 erläutert die Risikoanalyse auf Basis von IT-Grundschutz.

*BSI-Standard
100-1*

Der BSI-Standard 100-1 stellt als Elemente eines ISMS graphisch die Strategie, Management-Prinzipien, Ressourcen und Mitarbeiter dar. Strategie beschreibt er als Teil der Sicherheitsleitlinie, die ihrerseits Teil des IT-Sicherheitsprozesses ist. Letzterer enthält darüber hinaus die Themen IT-Sicherheitskonzept und IT-Sicherheitsorganisation.

Der Standard behält den Begriff IT-Sicherheit bei, weil er sich in der deutschen Literatur eingebürgert hat. Er führt jedoch aus, dass In-

formationssicherheit der angemessenere Begriff wäre, weil er unabhängig von den zugrunde liegenden Technologien und Medien ist.

Der Standard 100-1 geht u. a. auf den IT-Sicherheitsprozess ein. Er greift verschiedene Themen auf, die Lesern von „IT-Sicherheit mit System“ oder dem „Handbuch Unternehmenssicherheit“ seit längerem bekannt sind, so z. B. das Thema Lebenszyklus und der PDCA-Zyklus für den IT-Sicherheitsprozess.

Die Grundschutzkataloge stellen im Vergleich mit internationalen Normen und Practices aufgrund ihres Umfangs eine der Stärken des IT-GSHB des BSI dar. Mit den IT-GSK 2005 hat ein komprimierter und spezieller Lebenszyklus Eingang in die Bausteine gefunden. In den IT-GSK 2006 ist die System-Entwicklung als Maßnahme hinzugekommen. In der dreidimensionalen Sicherheitspyramide des Autors ist der Lebenszyklus einschließlich der sicherheitsorientierten Entwicklungsphase seit längerem integriert. Er ist umfangreicher und fachlich bedingt auch unterschiedlich zum BSI. Ferner erstreckt er sich über die Ressourcen hinaus auch auf Prozesse und Organisation.

*Vergleich zur
Sicherheits-
pyramide*

Die Sicherheitspyramide stellt darüber hinaus ein hierarchisches, umfassendes und durchgängiges Vorgehensmodell bereit, das sich auf das systematische Sicherheits-, Kontinuitäts- und Risiko- sowie Konformitätsmanagement von den Unternehmensanforderungen bis hin zu den Maßnahmen sowie über Prozesse, Personal und Ressourcen bis zur Organisation erstreckt. Zu den Ressourcen gehören auch ITK-Systeme. Die Sicherheitspyramide enthält außerdem Bedrohungskataloge sowie die Business und Operational Impact Analysis. Sicherheitsklassen und zugeordnete Sicherheitselemente runden sie ab. Zur Vereinheitlichung und Effizienzsteigerung unterscheidet die Sicherheitspyramide zwischen Richtlinien, Konzepten und Maßnahmen. Außerdem beinhaltet die Sicherheitspyramide den Sicherheitsregelkreis mit Kontrollelementen und Kennzahlen.

4.4.7 COBIT®, Version 4.0

Die Control Objectives for Information and related Technology (COBIT®) des IT Governance Institute® (ITGI®) und der Information Systems Audit and Control Association® (ISACA®) in Form des COBIT®-Frameworks unterstützen die IT-Governance. COBIT® [10] stellt ein Rahmenwerk zur Verfügung, um die IT auf die Geschäftstätigkeit auszurichten und den Gewinn zu maximieren. Außerdem hilft es dabei, IT-Ressourcen verantwortungsvoll zu nutzen und IT-Risiken angemessen zu steuern. COBIT® 4.0 bezeichnet sich als allgemein anerkanntes internes Kontroll-Rahmenwerk für die IT.

Als unterstützendes Referenzmaterial bei der Entwicklung von COBIT® 4.0 wurden angabegemäß u. a. folgende Normen und Practices verwendet: die ISO 17799:2005, ITIL®, die Reifegradmodelle CMM® und CMMI® sowie der Project Management Body of Knowledge (PMBOK®) des Project Management Institute®.

COBIT®-

Rahmenwerk

Das COBIT®-Rahmenwerk ist in Form eines dreidimensionalen Quaders dargestellt mit den Achsen geschäftliche Anforderungen in horizontaler Richtung, IT-Prozesse in vertikaler Richtung und IT-Ressourcen. Die geschäftlichen Anforderungen beziehen sich auf die Kriterien Effektivität, Effizienz, Vertraulichkeit, Integrität, Verfügbarkeit, Gesetzeskonformität (compliance) und Zuverlässigkeit von Informationen. Als IT-Ressourcen identifiziert COBIT® 4.0 die Anwendungen, die Informationen, die Infrastruktur und das Personal. Die IT-Prozesse sind unterteilt in die Ebenen Domänen, Prozesse und Aktivitäten.

COBIT®-

Prozessmodell

Das Prozessmodell von COBIT® unterscheidet die vier Domänen „planen und organisieren“, „beschaffen und implementieren“, „liefern und unterstützen“ sowie „überwachen und prüfen“. Es ähnelt damit den traditionellen Verantwortungsbereichen in der IT mit „plan“, „build“, „run“ und „monitor“. Die 4 Domänen beinhalten 34 generische Prozesse mit nun insgesamt 214 Aktivitäten. Für die Prozesse sind jeweils überblicksartige und detaillierte Kontrollziele angegeben sowie Kriterien für den Reifegrad.

COBIT®-

Domänen

Die Domäne „planen und organisieren“ enthält 10 Prozesse und behandelt neben strategischen und architekturellen Themenstellungen u. a. die Themenkomplexe Projektmanagement und Qualitätsmanagement sowie Personalmanagement. Die Domäne „beschaffen und implementieren“ behandelt z. B. die Beschaffung von IT-Ressourcen und das Releasemanagement.

Die Domäne „liefern und unterstützen“ enthält 13 und damit die meisten der 34 Prozesse. Unter den Prozessen finden sich Managementaufgaben, die auch von ITIL®, Version 2, bekannt sind, so z. B. aus dem dortigen Service Support das Ereignis-, Problem- und Konfigurationsmanagement und aus dem Service Delivery das Service-Level-Management, das Kapazitäts- und Performance-Management, sowie Themenstellungen, die sich mit dem Finanz-, Sicherheits- und Kontinuitätsmanagement beschäftigen. Der Fokus von COBIT® 4.0 liegt im Gegensatz zu ITIL®, das eine stärker prozessorientierte Sicht hat, auf den Kontrollen und dem Reifegrad. Was ist nun unter einer Kontrolle zu verstehen?

Betrachten wir hierzu aus der Domäne „liefern und unterstützen“ den Prozess zur Sicherstellung der Systemsicherheit. COBIT® 4.0 fordert als übergeordnetes Kontrollziel einen Sicherheitsmanagementprozess, um die Integrität der Informationen und den Schutz von IT-Ressourcen zu erreichen. Hierzu gehören – wie üblich – sowohl Rollen, Verantwortlichkeiten, Richtlinien und Verfahren als auch das Monitoring und Testen.

COBIT®-
Kontrollziele

Die nächste Ebene mit den detaillierteren Kontrollzielen geht auf die erforderlichen Aktivitäten dieses Prozesses und deren Inhalte ein. Beispielsweise soll sichergestellt sein, dass IT-Systeme vor Viren, Würmern, Spionagesoftware, aber auch betrügerischer unternehmensintern entwickelter Software geschützt sind. Messen lässt sich die Erfüllung der IT-Kontrollziele dieses Prozesses z. B. durch die Anzahl jener Systeme, welche die Sicherheitsanforderungen nicht erfüllen.

Die Stärke von COBIT® liegt in der Definition einer Vielzahl von Kontrollen, welche die Messbarkeit und damit Überwachung und Steuerung der IT-Prozesse unterstützen. Die Beschreibung der Prozesse selbst ist jedoch begrenzt. Demgegenüber bieten ITIL® und die ISO 20000 Beschreibungen für die Best Practices der Prozesse, während die Kontrollen weniger ausgeprägt sind.

COBIT®: Stärke

Die dreidimensionale Sicherheitspyramide enthält zusätzlich zu Kontrollen und Kennzahlen, die je nach Zielgruppe, deren hierarchischer Ebene und deren Informationsbedarf unterschiedlich sind, die Beschreibung der Sicherheitshierarchie sowie der Prozesse und Lebenszyklen. Die Sicherheitshierarchie ermöglicht die Ausrichtung des gesamten Unternehmens einschließlich seiner ITK auf die sicherheitsspezifischen geschäftlichen Anforderungen, also die Geschäftsziele, indem Prozesse, Ressourcen und Organisation (PROSim) genauso wie Produkte und Leistungen sowie Lebenszyklen auf diese Anforderungen ausgerichtet werden. Dies bezeichne ich als Business-Safety-Security-Continuity-Risk-Alignment, abgekürzt BuSSCRA bzw. BSSCRA.

Vergleich zur
Sicherheits-
pyramide

4.4.8 BS 25999-1:2006

Der britische Standard BS 25999-1:2006 enthält den Code of practice für das Business Continuity Management (BCM). Grundlage des BCM ist der BCM Lebenszyklus. Er enthält sechs Elemente.

Ausgangspunkt ist die BCM-Politik. Sie definiert zwei Prozesse, deren einer anfangs zur Etablierung der Fähigkeit zur Geschäftskontinuität erforderlich ist, während der andere zum fortlaufenden Ma-

nagement und zur Pflege der Fähigkeit zur Geschäftskontinuität notwendig ist. Die BCM-Politik sollte Aussagen enthalten zum Geltungsbereich, zu den Ressourcen, den Prinzipien, Richtlinien und minimalen Standards der Organisation sowie zu relevanten Standards und Regularien.

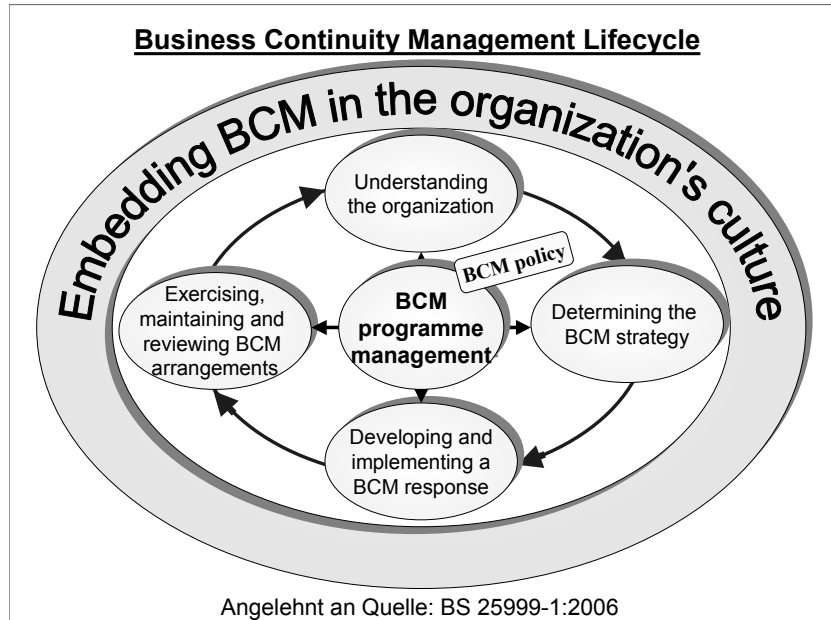


Abb. 4.3: BCM Lifecycle

*BCM-
Programm-
management
etablieren*

Das erste Element, nämlich den zentralen steuernden Kern des BCM-Prozesses, bildet das BCM-Programmmanagement. Es enthält drei Schritte: die Zuordnung von Verantwortlichkeiten, die Implementierung der Geschäftskontinuität in der Organisation und das fortwährende Management der Geschäftskontinuität.

*Das
Unternehmen
und seine
Anforderungen
verstehen*

Die erste Phase des Lebenszyklus besteht darin, die Organisation und ihre Anforderungen zu verstehen. Dies beinhaltet die Kenntnis der Ziele der Organisation und ihrer Bezugsgruppen sowie ihres Umfeldes. Die Aktivitäten und Ressourcen der Organisation sind zu identifizieren. Anschließend sind die Auswirkungen einer Unterbrechung mittels einer Business Impact Analysis (BIA) zu erheben. Kritische Aktivitäten und Kontinuitätsanforderungen sind zu bestimmen. Mit Hilfe einer Risikoanalyse (RA) orientiert an ISO 27001 sind Bedrohungen kritischer Aktivitäten zu bewerten. Mögliche Gegenmaßnahmen sind festzulegen. Das Top Management ist gefordert, die

geschäftskritischen Produkte und Leistungen sowie BIA und RA zu unterzeichnen.

In der zweiten Phase legt die Organisation ihre BC-Strategie fest. Strategien beziehen sich z. B. auf Personen, Technologien und Informationen. Sie umfassen Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit von Ereignissen oder deren Auswirkungen sowie die Kontinuität kritischer Aktivitäten. Ausweichstandorte sowie Vereinbarungen mit Dritten sind Teil der Strategie. Das Top Management sollte die Strategien abzeichnen.

*BC-Strategie
festlegen*

Die dritte Phase widmet sich der Entwicklung von Plänen und der Implementierung von Maßnahmen zur Erhaltung der Geschäftskontinuität. Eine Organisationsstruktur sollte festgelegt sein, um ein Ereignis beurteilen und unter Kontrolle bekommen zu können sowie die Kommunikation mit den Bezugsgruppen herzustellen. Für die Anfangsphase eines Notfalls sollte ein Incident-Management-Plan (IMP) aufgestellt sein. Zu den ersten Maßnahmen gehört die Sicherheit von Personen. Hierzu gehört die Gebäuderäumung sowie die Mobilisierung von Erste-Hilfe- und Evakuierungsteams. Notfallpläne (Business Continuity Plans {BCP}) enthalten Maßnahmen zum Wiederanlauf der Geschäftsaktivitäten nach einer Unterbrechung.

*Geschäfts-
kontinuität
planen und
Maßnahmen
einführen*

Phase 4 widmet sich der Übung, der Pflege und Überprüfung des BCM. Ein Übungsprogramm sollte u. a. die technischen, logistischen und prozeduralen Systeme des Notfallplans sowie Rollen und Verantwortlichkeiten beinhalten. Die Übungsziele sollten klar definiert sein. Hinsichtlich der Wartung sollte ein formaler Änderungsprozess etabliert sein. Das Top Management sollte die BCM-Fähigkeiten der Organisation in angemessenen Intervallen überprüfen.

*üben, pflegen,
überprüfen*

Als übergreifendes Element ist BCM in die Organisationskultur einzubinden. Schulungen, Übungspläne und BCM-Bewusstsein (awareness) unterstützen die Einbindung.

Die dreidimensionale Sicherheitspyramide, die das Kontinuitätsmanagement enthält, geht ebenfalls von einer Politik aus, die jedoch umfassender gestaltet ist, indem sie Sicherheit und Risiko mit betrachtet. Die nächste Ebene der Sicherheitspyramide erhebt die Anforderungen der Geschäftsprozesse im Rahmen einer Geschäftseinflussanalyse auf Basis der Geschäftsprozessarchitektur. Dies ist vergleichbar mit dem ersten Schritt des BCM-Lebenszyklus. Die Transformationsebene bildet diese Anforderungen auf Produkte, Leistungen, Prozesse und Ressourcen ab, ähnlich der BCM-Strategie der BS 25999-1:2006. Den Überblick über Produkte, Leistungen, Pro-

*Vergleich zur
Sicherheits-
pyramide*

zesse und Ressourcen sowie Bedrohungen, Schutzbedarf und Risiken gibt die Architekturebene der Sicherheitspyramide.

Der dritten Phase im BCM-Lebenszyklus mit der Entwicklung von Plänen und der Implementierung von Maßnahmen entsprechen in der Sicherheitspyramide drei Ebenen. Dies sind die Ebene der Richtlinien und generischen Konzepte mit z. B. Vorlagen für Notfallpläne, die darauf aufbauenden spezifischen Konzepten in Form spezifischer Notfallpläne sowie die Maßnahmenebene.

Dem BCM-Programmmanagement entspricht der Sicherheitsmanagementprozess zusammen mit dem Sicherheitsregelkreis.

Gegenüber der BS 25999-1:2006 betrachtet die Sicherheitspyramide zusätzlich den Lebenszyklus von Produkten, Leistungen, Prozessen und Ressourcen sowie die Begleitprozesse bzw. Managementdisziplinen.

4.4.9 BS 25999-2

In Planung für das Jahr 2007 befindet sich der britische Standard BS 25999-2, Business Continuity Management, Part 2: Specification. Er soll Anforderungen zum Aufbau und zur effektiven Steuerung eines Business Continuity Management Systems (BCMS) definieren.

Der Entwurf vom 15. Juni 2007 betont, wie wichtig es ist, die Anforderungen des Unternehmens an die Geschäftskontinuität zu verstehen und Kontrollen zu implementieren und zu betreiben. Leistungsfähigkeit und Effektivität des BCM müssen beobachtet und geprüft werden. Der kontinuierliche Verbesserungsprozess schließlich muss auf objektiven Messergebnissen basieren.

BCMS

Das BCMS besteht demzufolge aus klar zugeordneten Verantwortlichkeiten und dem Managementprozess, der von der BCM-Politik ausgeht, Planung, Implementierung und Betrieb beinhaltet, die Leistungsfähigkeit bewertet, Verbesserungen vornimmt und ein Management Review vorsieht. Ein BCMS umfasst weiterhin auditierbare Unterlagen und spezifische Vorgehensweisen, z. B. für die Durchführung einer Business Impact Analysis und die Erstellung von Business Continuity Plans (BCPs).

PDCA-Zyklus

Nicht zuletzt aus Gründen der Konsistenz mit anderen Standards für Management Systeme, wie z. B. ISO 9001:2000, ISO 20000-2:2005 und ISO 27001:2005 verwendet BS 25999-2 den PDCA-Zyklus für ein BCMS.

Das dreidimensionale Pyramidenmodell nach Dr.-Ing. Müller stellt ein systematisches und integratives Managementmodell dar. Es integriert u. a. das Sicherheits-, Kontinuitäts- und Risikomanagement. Ausgangspunkt ist auch hier die Ebene der Politik, die jedoch umfassender gestaltet ist. Die nächste Ebene der Sicherheitspyramide erhebt die Anforderungen der Geschäftsprozesse im Rahmen einer Geschäftseinflussanalyse (Business Impact Analysis). Ausgangspunkt ist die – wie der Autor es nennt – Unternehmensarchitektur, bestehend u. a. aus Prozessen, Ressourcen und Organisation sowie Produkten und Dienstleistungen. Richtlinien und Vorlagen z. B. für die Durchführung einer Business Impact Analysis oder die Entwicklung von BCPs sind ebenfalls enthalten. Der Kontinuitätsmanagementprozess orientiert sich ebenfalls am PDCA-Zyklus.

Vergleich zur Sicherheits- bzw. Kontinuitätspyramide

Gegenüber dem Entwurf der BS 25999-2:2007 betrachtet die Sicherheitspyramide zusätzlich den Lebenszyklus von Produkten, Leistungen, Prozessen und Ressourcen sowie die Begleitprozesse bzw. Managementdisziplinen.

4.4.10 Fazit: Normen und Practices versus Sicherheitspyramide

Die genannten Normen und Practices unterscheiden sich in ihrem Fokus und in den Abstraktionsebenen, die häufig jedoch überblicksartig sind. Dementsprechend weisen sie unterschiedliche Ansätze und Stärken auf. Die Herausforderung für den Praktiker besteht darin, diese verschiedenen Ansätze und Stärken zusammenzuführen.

Herausforderung für den Praktiker

Das hierfür erforderliche durchgängige, systematische und praxisorientierte Vorgehensmodell für das integrative Sicherheits-, Kontinuitäts- und Risikomanagement in Unternehmen bietet die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller. Sie umfasst die Sicherheitshierarchie, die IT-Prozesse einschließlich des IT-Sicherheitsmanagementprozesses, die Ressourcen und die Organisation bis hin zum Lebenszyklus von Prozessen, Ressourcen, Produkten und Dienstleistungen sowie das Monitoring und Controlling mit entsprechenden Kennzahlen.

Lösung: Normen-übergreifende und integrative Sicherheit mit der dreidimensionalen Sicherheitspyramide

Sie vereinigt daher schon seit vielen Jahren ([5], [6], [7]) Vorgehens-elemente und Themen, die in unterschiedlicher Tiefe, Ausprägung und Konkretisierung sowie verteilt auch in aktuellen Normen und Practices enthalten sind. Zu diesen Normen und Practices im ITK-Bereich gehören die ISO 13335-1:2004, die ISO 17799:2005, die ISO 27001:2005, ITIL® und COBIT®, BS 25999 sowie das IT-GSHB des BSI. Ein weiteres Element ist die Balanced Scorecard [11]. Konkrete Richtlinien, Konzepte und Maßnahmen stellen den Praxisbezug der dreidimensionalen Sicherheitspyramide des Autors her. Sie ist Vorreiter

für systematisches, integratives, prozess-, produkt-, leistungs- und lebenszyklusimmanentes Sicherheits-, Kontinuitäts- und Risikomanagement. Sie ist im vorliegenden Buch mit ihrer Vorgehensweise sowie zahlreichen wichtigen Beispielen und Details beschrieben. Dennoch sind viele weitere Inhalte und Hilfsmittel der dreidimensionalen Sicherheits-, Kontinuitäts- und Risikomanagementpyramide hier nicht dokumentiert, da sie den Rahmen eines Buchs sprengen würden.

Business-Safety-Security-Continuity-Risk-Alignment

Durch die Methodik der dreidimensionalen Sicherheitspyramide können Sie die häufig unter dem Thema „Business-ICT-Alignment“ angesprochene Konsistenz zwischen den Anforderungen des Unternehmens und seiner ITK im Hinblick auf Sicherheit, Kontinuität und Risiko herstellen und zwar sowohl für die IT als auch für die Non-IT (s. „Handbuch Unternehmenssicherheit“). Die Sicherheitspyramide ermöglicht hierbei den Aufbau einer umfassenden und durchgängigen Konsistenz zwischen den sicherheitsspezifischen Geschäftszielen des Unternehmens und all seinen Prozessen und Ressourcen, seinen Produkten und Dienstleistungen sowie seiner Organisation und den Lebenszyklen. Dies bezeichne ich umfassend als Business-Safety-Security-Continuity-Risk-Alignment (BSSCRA) bzw. BuSSeCoRA oder auch integrierend kurz: Business-Safety-Security-Alignment (BSSA {B, double S, A}) bzw. noch prägnanter Business-Security-Alignment (BSA).

Die Tabelle gibt einen auszugsweisen Überblick, welche Normen und Practices sich auf welche Elemente der Sicherheitspyramide beziehen. Die Kreuze machen jedoch keinerlei Aussage zum jeweiligen Umfang, Detaillierungsgrad oder zur jeweiligen Qualität, letzteres z. B. hinsichtlich des jeweils angewandten Vorgehensmodells.

Business-Enterprise-Alignment

Wer darüber hinaus die Ausrichtung des Gesamtunternehmens mit all seinen Prozessen, Ressourcen, Produkten, Dienstleistungen und Lebenszyklen sowie seiner Organisation auf die Geschäftsziele erreichen möchte, kann dies mit der bereits erwähnten Unternehmenspyramide bzw. Unternehmensmanagementpyramide nach Dr.-Ing. Müller. Dies bezeichne ich als Business-Process-Ressource-Organisation-Product-Service-and-Lifecycle-Alignment (BuPROPSeLiA). Als Kurzform habe ich den Begriff Business Enterprise Alignment (BEA, BEntA) bzw. Business Enterprise Linkage (BEL) geprägt.

Norm, Standard, „practice“	Hierarchie						PRO	Sim	L	CON	PDCA		
	Politik	Anforderungen	Transformation	Architektur	Richtlinien	Konzepte	Maßnahmen	Prozesse	Ressourcen	Organisation	Lebenszyklus	Monitoring, Controlling Reporting, Auditing	Sicherheitsprozess, PDCA-Zyklus
ISO 13335													
- corporate security policy	X												
- information security policy	X												
- corporate ICT security policy	X												
- ICT system security policy					X								
- Organizational aspects	X				X					X			
ISO 17799, 27002:2005													
- Risk Assessment and Treatment			X	X									
- Security Policy	X									X			
- Organization of Information Security	X									X			
- Asset Management		X		X						X			
- Human Resources Security									X				
- Physical and Environmental Security					X			X	X				
- Communications and Operations Management					X			X			X	X	
- Access Control					X								
- Information Systems Acquisition, Development and Maintenance					X						X		
- Information Security Incident Management				X				X					
- Business Continuity Management				X				X					
- Compliance	X			X				X				X	

4 Definitionen zum Sicherheits-, Kontinuitäts- und Risikomanagement

Norm, Standard, „practice“	Hierarchie							PROSim		L	CON	PDCA	
	Politik	Anforderungen	Transformation	Architektur	Richtlinien	Konzepte	Maßnahmen	Prozesse	Ressourcen	Organisation	Lebenszyklus	Monitoring, Controlling, Reporting, Auditing	Sicherheitsprozess, PDCA-Zyklus
ISO 27001												X	X
...													
ITIL®, Version 2				X				X	X				
- Incident Management				X				X	X				
- Problem Management				X				X	X				
- Change Management				X				X	X				
- Release Management				X				X	X				
- Configuration Management				X				X	X				
- Service Level Management				X				X	X				
- Financial Management				X				X	X				
- Capacity Management				X				X	X				
- Availability Management				X				X	X				
- Continuity Management				X				X	X				
- Security Management				X				X	X				
- ICT Infrastructure Management				X				X	X				
- Application Management				X				X	X				
ISO 20000				X				X	X				
...													
COBIT®, Version 4.0								X				X	
...													
IT GSHB	X				X	X			X	X	X		X
...													

4.5 Ingenieurmäßige Sicherheit – Safety, Security, Continuity Engineering

Unter ingenieurmäßiger Sicherheit einschließlich Kontinuität verstehe ich ein Sicherheitsmanagementsystem,

- dessen Aufbau einer systematischen Vorgehensweise folgt
- das Rahmenbedingungen wie z. B. Gesetze, Regularien und Normen berücksichtigt
- das Methoden nutzt und Lebenszyklen berücksichtigt
- das effizient, strukturiert, praxisorientiert und ganzheitlich ist.

Ganzheitlichkeit geht hierbei über die losgelöste Betrachtung einzelner Komponenten und die Schaffung von Insellösungen hinaus, indem sie das gesamte Unternehmen und sein Umfeld betrachtet. Sie berücksichtigt den Schutz gegenüber Angriffen (Security), die Betriebssicherheit (Safety) einschließlich des Schutzes vor Naturgewalten sowie den Schutz vor Notfällen und Katastrophen (Continuity). Außerdem erfordert ein ganzheitliches ingenieurmäßiges Vorgehen neben der Betrachtung technologischer Aspekte die Berücksichtigung prozessualer, ressourcenspezifischer und organisatorischer Elemente. Ein weiterer Aspekt ist der Lebenszyklus von Prozessen und Ressourcen sowie Produkten und Leistungen (services), der ebenfalls in die Vorgehensweise zu integrieren ist.

In Anlehnung an den Begriff Security Engineering [12] bezeichne ich ingenieurmäßige Sicherheit [13] auch als Safety and Security Engineering bzw. Safety, Security and Continuity Engineering (SSCE).

Die Sicherheitspyramide nach Dr.-Ing. Müller, die im folgenden Unterkapitel überblicksartig dargestellt ist, verkörpert ein Vorgehensmodell für das Safety, Security and Continuity Engineering.

*Safety,
Security and
Continuity
Engineering*

*Sicherheits-
pyramide*

4.6 Sicherheitspyramide

Die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller, die auch als Sicherheitsmanagementpyramide nach Dr.-Ing. Müller bezeichnet werden kann, ist ein systematisches, ganzheitliches und praxisorientiertes Vorgehensmodell für den Aufbau, die Überprüfung und kontinuierliche Fortentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements eines Unternehmens. Sie dient gleichzeitig der transparenten Visualisierung der Vorgehensweise. Die fünfstufige Sicherheitspyramide [5] entwickelte der Autor inzwischen zur siebenstufigen Sicherheitspyramide fort. Sie besitzt die drei Dimensionen Sicherheitshierarchie, PROSim (Prozesse, Ressourcen und

Organisation für das Sicherheitsmanagement) und den Lebenszyklus von Prozessen und Ressourcen sowie Produkten und Dienstleistungen. Ein Regelkreis und der Sicherheitsprozess dienen der Steuerung und Weiterentwicklung.

Die Sicherheitspyramide stellt somit ein ingenieurmäßiges Vorgehen im Sinne des Safety and/or Security and/or Continuity Engineering dar.

Das Dilemma

Doch warum sollten Unternehmen in Anbetracht knapper Budgets und wenig Personals die derzeitigen Insellösungen aufgeben? Weil die externen Anforderungen, z. B. durch EuroSOX, KonTraG, Basel II, und MaRisk steigen, die Bedrohungen durch Viren, globalen Wettbewerb und Terrorismus zunehmen und gegebenenfalls das Risiko der persönlichen Haftung besteht. Doch wie können Sie das Dilemma zwischen knappen Budgets einerseits und höheren Anforderungen und stärkeren Bedrohungen andererseits lösen?

*Software-Krise
der 60er Jahre
als Vergleich*

Diese vielerorts anzutreffende Lage zeigt Parallelen zur Software-Krise Ende der 60er Jahre. Erst durch das Software-Engineering konnte hier ein Ausweg gefunden werden. Dementsprechend ist jetzt in der Sicherheit ingenieurmäßiges Vorgehen angesagt. Sicherheit sollte hierbei praxisorientiert, systematisch und wirtschaftlich aufgebaut und weiterentwickelt werden. Anerkannte Standards, Methoden und Werkzeuge geben dabei Orientierung. Hierzu gehören im IT- bzw. ITK-Bereich Normen wie die ISO 13335, die ISO 17799, die ISO 27000-Reihe, aber auch Best Practices à la ITIL®, die Maßnahmen des BSI-IT-Grundschutzhandbuchs und COBIT®. Das Ergebnis muss ganzheitlich und gleichzeitig schlank sein. Denn wer hat heutzutage noch die Zeit, dicke unternehmensspezifische Wälzer zu lesen?

*Ganzheitlichkeit
– ein
Widerspruch?*

Ganzheitlichkeit scheint da ein Widerspruch zu sein. Sie bedeutet eine Abkehr von der rein technischen Sichtweise. Prozessuale, ressourcenspezifische, technologische, methodische, personelle und organisatorische Elemente sind zusätzlich zu berücksichtigen. Die Budgetverantwortlichen sehen diese ergänzenden Elemente, assoziieren damit zusätzliche Kosten und stellen kritische Fragen. Wie lassen sie sich überzeugen?

*Hausbau –
ein Vergleich*

Vielleicht durch einen Vergleich mit der über Jahrhunderte bewährten Baukunst? Können Sie sich vorstellen, einen Architekten mit einem Hausentwurf zu beauftragen, ohne ihm die Rahmenbedingungen zu nennen? Größe, Ausstattung, Lage, Zeitplan und Budget sollten zumindest erste Eckpunkte sein. Andernfalls verwerfen Sie einen Entwurf nach dem anderen. Das verschwendet Zeit und Geld. Sicherlich haben Sie auch Vorstellungen zur Sicherheit Ihres geplanten

Hauses. Wollen Sie Standardfenster oder abschließbare, oder soll das Glas auch einbruchhemmend sein? Wollen Sie eine Einbruchmeldeanlage, Bewegungsmelder, Überwachungskameras, einen Safe? Je genauer Sie die Rahmenbedingungen vorgeben, desto zielgenauer und effizienter kann die Lösung ausfallen. Lassen Sie das Haus schließlich bauen, so erfolgt dies nach einem Zeitplan und unter ständiger Überwachung und Steuerung durch die Bauleitung. Doch selbst wenn Sie alle Ihre Sicherheitsanforderungen haben realisieren lassen, nützt das nichts, wenn die Fenster über Nacht offen stehen, weil die Hausbewohner sie zu schließen vergessen haben: Mangelndes Sicherheitsbewusstsein. Was zeigt uns das?

Vorgaben, Planung und Steuerung sowie eine ganzheitliche Betrachtung aller Sicherheitsaspekte vermeiden Doppelarbeiten und ermöglichen eine zielgerichtete und damit effiziente Steuerung. Die Sorge vieler Geschäftsleiter, dass sich Sicherheit verselbständigt und zu einem unkontrolliert teuren Etwas wird, wird so begrenzt.

Konkrete Beispiele bestätigen dies. So erarbeiteten und entwickelten in verschiedenen Unternehmen die Geschäftsbereiche ihre Notfall- und Katastrophenvorsorgepläne individuell. Eine Vorgabe zu Struktur und Inhalten gab es nicht. So erfanden die Geschäftsbereiche das „Rad“ zu Lasten der Wirtschaftlichkeit immer wieder neu und in unterschiedlicher Qualität und Vollständigkeit.

*Konkrete
Beispiele*

Ein anderes Beispiel lieferten sicherheitstechnisch miteinander vergleichbare IT-Systeme. Hier entwickelten die Verantwortlichen deren Schutzmaßnahmen nach bestem Wissen und Gewissen, aber individuell. In der Folge waren die IT-Systeme trotz gleicher Anforderungen unterschiedlich gut abgesichert. Dies führte zu Sicherheitsdefiziten und machte Nachbesserungen erforderlich.

4.7 Sicherheitspolitik

Den Begriff Sicherheitspolitik bzw. Sicherheitsleitlinie definieren verschiedene Normen, Standards und Publikationen unterschiedlich. Die folgenden Unterkapitel geben einen Auszug dieser Definitionen wieder, bevor die in diesem Buch verwendete Definition des Autors dargestellt wird.

4.7.1 ... nach IT-Grundschriftbuch/-katalogen (IT-GSHB 2006)

Seit der Ausgabe 2005 ist das IT-Grundschriftbuch (IT-GSHB) des BSI unterteilt in die Grundschrift-Vorgehensweise und die IT-Grundschriftkataloge (IT-GSK). Die IT-GSK 2006 erläutern in M 2.192,

*IT-Sicherheits-
leitlinie*

Erstellung einer IT-Sicherheitsleitlinie, dass diese die Leitaussagen zur IT-Sicherheitsstrategie zusammenfassen sollte. Sie soll die „IT-Sicherheitsziele und das angestrebte Sicherheitsniveau für alle Mitarbeiter“ dokumentieren. Gleichzeitig bekennt sich die Unternehmensleitung damit „sichtbar zu ihrer Verantwortung für die IT-Sicherheit“. Gemäß M 2.201 ist die IT-Sicherheitsleitlinie eine Dokumentation im Rahmen des IT-Sicherheitsprozesses.

Die IT-Sicherheitsleitlinie soll laut IT-GSK 2006, M 2.192, kurz und übersichtlich sein und u. a. folgende Themen ansprechen:

- Stellenwert der IT-Sicherheit
- IT-Sicherheitsziele und deren Bezug zu den Geschäftszielen
- Kernelemente der IT-Sicherheitsstrategie
- Verpflichtung der Leitungsebene
- Organisationsstruktur zur Umsetzung des IT-Sicherheitsprozesses

(IT-)
Sicherheits-
leitlinien für
Sicherheits-
gateway und
Faxserver

Zusätzliche (IT-)Sicherheitsleitlinien der IT-GSK 2006 beziehen sich auf technische Komponenten, wie z. B. Sicherheitgateways (M 2.299) und Faxserver (M 2.178). Im Baustein B 3.301, Sicherheitgateway (Firewall), erläutern die IT-GSK, dass ein Sicherheitgateway die „technisch mögliche auf die in einer IT-Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation“ einschränkt.

Politik,
Leitlinie,
Richtlinie

Gemäß Glossar der IT-GSK 2006 betrachtet das BSI den Begriff Sicherheitspolitik als falsche Übersetzung von „Security Policy“ und verweist auf Sicherheitsrichtlinie als Übersetzung von „Security Policy“. Die Maßnahme M 2.39 beschäftigt sich mit der Reaktion auf Verletzungen der Sicherheitspolitik, die Maßnahme M 2.71 mit der Festlegung einer Policy für ein Sicherheitgateway. Der BSI-Standard 100-1, Version 1.0, bietet als Übersetzung von „Security Policy“ den Begriff IT-Sicherheitsleitlinie an.

4.7.2 ... nach ITSEC

In den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) [14] sind drei unterschiedliche Arten der Sicherheitspolitik prinzipiell wie folgt definiert:

Firmen-
spezifische
Sicherheits-
politik

Firmenspezifische Sicherheitspolitik: „Die Sammlung von Gesetzen, Regeln und Praktiken, die vorschreiben, in welcher Weise Vermögenswerte einschließlich sensibler Informationen innerhalb einer Benutzerorganisation behandelt, geschützt und verteilt werden.“

System-Sicherheitspolitik: „Die Sammlung von Gesetzen, Regeln und Praktiken, die vorschreiben, in welcher Weise sensitive Informationen und andere Betriebsmittel innerhalb eines bestimmten Systems behandelt, geschützt und verteilt werden.“

*System-
Sicherheits-
politik*

Technische Sicherheitspolitik: „Die Menge der Gesetze, Regeln und Praktiken, die die Verarbeitung von sensitiven Informationen und die Nutzung von Betriebsmitteln durch die Hard- und Software eines IT-Systems oder –Produkts festlegen.“

*Technische
Sicherheits-
politik*

Die hier definierten Sicherheitspolitiken beinhalten demzufolge Gesetze, Regeln und Praktiken.

4.7.3 ... nach ISO/IEC 13335-1:2004

Die ISO/IEC 13335-1:2004 unterscheidet zwischen vier Arten der Sicherheitspolitik:

- Unternehmensweite Sicherheitspolitik (corporate security policy)
- Informationssicherheitspolitik (information security policy)
- Unternehmensweite ITK-Sicherheitspolitik (corporate ICT security policy)
- Sicherheitspolitik des ITK-Systems (ICT system security policy).

Diese sind in der ISO/IEC 13335-1:2004 prinzipiell wie folgt definiert:

„Die unternehmensweite Sicherheitspolitik (corporate security policy) kann die Sicherheitsprinzipien und -direktiven für die Organisation als Ganzes beinhalten. Die unternehmensweite Sicherheitspolitik sollte die breitbandigere Unternehmenspolitik widerspiegeln einschließlich der Elemente, die Persönlichkeitsrechte, gesetzliche Anforderungen und Standards adressieren.“

*Unternehmens-
weite
Sicherheits-
politik*

„Die Informationssicherheitspolitik kann Prinzipien und Direktiven enthalten, die für den Schutz jener Informationen spezifisch ist, die sensibel oder wertvoll oder in anderer Hinsicht für die Organisation wichtig sind.“

*Informations-
sicherheits-
politik*

„Die unternehmensweite ITK-Sicherheitspolitik sollte sowohl die grundlegenden Sicherheitsprinzipien und -direktiven widerspiegeln, die sich aus der unternehmensweiten Sicherheitspolitik und der Informationssicherheitspolitik ergeben, als auch den generellen Einsatz von ITK-Systemen innerhalb der Organisation.“

*Unterneh-
mensweite ITK-
Sicherheits-
politik*

„Die Sicherheitspolitik eines ITK-Systems sollte jene Sicherheitsprinzipien und -direktiven widerspiegeln, die in der unternehmensweiten ITK-Sicherheitspolitik enthalten sind. Sie sollte darüber hinaus Details der spezifischen Sicherheitsanforderungen enthalten sowie

*Sicherheits-
politik eines
ITK-Systems*

der Schutzmaßnahmen (safeguards), die implementiert werden müssen, einschließlich deren korrekte Nutzung, um eine adäquate Sicherheit zu erreichen. In jedem Fall ist es wichtig, dass der gewählte Ansatz im Hinblick auf die Geschäftsanforderungen der Organisation effektiv ist.“

Die ISO/IEC 13335-1 nutzt einen hierarchischen Ansatz, der vier unterschiedliche Arten der Sicherheitspolitik definiert. Entscheidend ist, dass der Ausgangspunkt die Anforderungen des Unternehmens sind.

4.7.4 ... nach ISO 15408 (Common Criteria)

Im Glossar der ISO 15408 [15], Teil 1, bzw. den Common Criteria, Version 2.3 [16], Teil 1, wird zwischen der Sicherheitspolitik des Evaluationsgegenstandes (EVG) und der Funktionalen Sicherheitspolitik unterschieden.

EVG-Sicherheitspolitik

Die EVG-Sicherheitspolitik umfasst demzufolge die „Menge von Regeln, die angibt, wie innerhalb eines Evaluationsgegenstands Werte verwaltet, geschützt und verteilt werden“.

Funktionale Sicherheitspolitik

Die Funktionale Sicherheitspolitik ist definiert als „Sicherheitspolitik, die durch eine Sicherheitsfunktion durchgesetzt wird“.

In den Common Criteria V3.1 vom September 2006, die der ISO zur Standardisierung vorliegen, ist die funktionale Sicherheitspolitik (security function policy) definiert als eine „Menge von Regeln, die das spezifische Sicherheitsverhalten beschreiben, das durch Sicherheitsfunktionen des Evaluationsgegenstandes durchgesetzt wird, und die sich als Menge von Anforderungen an Sicherheitsfunktionen ausdrücken lassen“.

Organisatorische Sicherheitspolitik

Die Common Criteria V3.1 kennen zusätzlich eine organisatorische Sicherheitspolitik (organisational security policy). Sie stellt „eine Menge von Sicherheitsregeln, Verfahren oder Richtlinien dar, die jetzt und/oder zukünftig durch eine aktuelle oder hypothetische Organisation in der Betriebsumgebung eingeführt (oder voraussichtlich eingeführt) werden“.

Die ISO bzw. die Common Criteria verstehen die Sicherheitspolitik demzufolge im Sinne von Regeln, die von dem Evaluationsgegenstand bzw. Sicherheitsfunktionen umgesetzt werden. Die CC V3.1 kennen zusätzlich eine organisatorische Sicherheitspolitik.

4.7.5 ... nach ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005

In der ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005 ist die Informationssicherheitspolitik wie folgt beschrieben:

Ziel der Informationssicherheitspolitik (information security policy) ist es, dass das Management die Ausrichtung im Hinblick auf die Informationssicherheit vorgibt und sie unterstützt.

*Informations-
sicherheits-
politik*

Das Management sollte zum einen eine klare Ausrichtung der (Sicherheits)politik festlegen. Zum anderen sollte es die Informationssicherheit unterstützen und sich auf sie verpflichten, indem es die Informationssicherheitspolitik für die gesamte Organisation herausgibt und pflegt.

4.7.6 ... nach ISO/IEC 27001:2005

Die ISO/IEC 27001:2005 bezeichnet die Informationssicherheitspolitik als Politik des Informationssicherheitsmanagementsystems (ISMS-Politik). Sie gibt im Hinblick auf Informationssicherheit eine überblicksartige Orientierung und berücksichtigt dabei geschäftliche, gesetzliche und vertragliche Verpflichtungen. Sie stellt den Bezug zum strategischen Risikomanagement her. Das Management gibt die ISMS-Politik frei.

ISMS-Politik

4.7.7 ... nach Dr.-Ing. Müller

In der Sicherheitspolitik, genauer der Sicherheits-, Kontinuitäts- und Risikopolitik, eines Unternehmens legt das Top Management in schriftlicher überblicksartiger Form fest, welche Bedeutung und Ausprägung das Thema Sicherheit einschließlich Kontinuität für das Unternehmen haben soll. Hierbei spielen Aussagen zur Risikotragfähigkeit und Risikofreudigkeit eine wesentliche Rolle. Die Sicherheitspolitik leitet sich aus der Unternehmenspolitik ab. Letztere beinhaltet die Vision, den Zweck, die Ziele und die Strategie des Unternehmens. Sie basiert auf den unterschiedlich gewichteten Anforderungen der Bezugsgruppen (Kunden, Anteilseigner, Mitarbeiter, Lieferanten, Öffentlichkeit, Staat {z. B. Gesetze, Vorschriften} etc.) sowie dem Selbstverständnis und der Strategie des Unternehmens.

*Sicherheits-
politik*

In der Sicherheitspolitik verpflichtet sich das Management zur Übernahme seiner Verantwortung für die Unternehmenssicherheit. Dies beinhaltet die Festlegung eines Orientierungsrahmens und die anschließende Umsetzung und Einhaltung der selbst auferlegten Regularien sowie die Bereitstellung der erforderlichen Mittel und Ressourcen.

Die Sicherheitspolitik ist somit nicht spezifisch auf die ITK ausgerichtet, sondern im Sinne einer unternehmensweiten Sicherheitspolitik zu verstehen. Dies betont, dass der Ausgangspunkt jeglicher Sicherheit die Anforderungen des Unternehmens sind. Die Sicherheitsanforde-

rungen der ITK leiten sich hieraus ab. Dies fördert das Business-Security-Alignment, genauer das Business-Safety-Security-Continuity-Risk-Alignment.

*Parallelen zur
Sicherheits-
pyramide*

Die oberste Ebene der Sicherheitspyramide, die Sicherheitspolitik, hat ihre Analogie in der unternehmensweiten Sicherheitspolitik der ISO/IEC 13335-1 und der Sicherheitspolitik der ISO/IEC 17799:2005. Der prinzipielle hierarchische Ansatz der ISO/IEC 13335-1 spiegelt sich in ähnlicher, aber detaillierterer Form in der Sicherheitspyramide wider. Hierbei findet die unternehmensweite ITK-Sicherheitspolitik der ISO/IEC 13335-1 ihre Entsprechung in den – allerdings vielfältigeren – Sicherheitsrichtlinien der Sicherheitspyramide. Die Sicherheitspolitik des IT-Systems hat ihre Parallele in den Sicherheitskonzepten.

Die Ende 2005 erschienene ISO/IEC 27001 formuliert ein ähnliches Verständnis der dort ISMS-Politik genannten Sicherheitspolitik, wie sie zuvor bereits in der ersten Auflage von „IT-Sicherheit mit System“ angegeben war. Die Autoren der Norm merken an, dass sie die ISMS-Politik als Obermenge der Informationssicherheitspolitik ansehen. Die ISO/IEC 27001 bezieht das Risikomanagement in die ISMS-Politik mit ein, wie es in der zurückliegenden zweiten Auflage dieses Buchs angegeben war.

*Politik,
Leitlinie,
Richtlinie*

Ebenso wie bei der ISO/IEC 13335-1 gibt es aus meiner Sicht keine Beschränkungen in der Verwendung der Begriffe Politik, Richtlinie oder Leitlinie für das Unternehmen, seine Bereiche oder Ressourcen. Um im Deutschen Verwechslungen zwischen Leitlinie und Richtlinie zu vermeiden, empfehle ich die Verwendung des Begriffs Politik als oberste Ebene und des Begriffs Richtlinie als konkretere aber übergreifende Vorgabe. Die Verwendung des Begriffs Politik finden Sie neben Sicherheitspolitik z. B. auch in den Wörtern Risikopolitik, Unternehmenspolitik, Arbeitsmarktpolitik, etc. Laut DUDEN, Das große Fremdwörterbuch, 2. Auflage, 2000, ist ...politik ein „Wortbildungselement mit der Bedeutung „Gesamtheit von Bestrebungen mit bestimmter Aufgabenstellung und Zielsetzung im Hinblick auf das im ersten Bestandteil der Zusammensetzung Genannte““.

4.7.8 Vergleich

Die unterschiedlichen Definitionen der Sicherheitspolitik sind in der folgenden Tabelle überblicksartig vergleichend dargestellt:

Kategorisierung der Definitionen zur Sicherheitspolitik/ Sicherheitsleitlinie		
Quelle	Überblicksartige Unternehmens-/ Managementvorgaben	Richtlinien, Regeln, Praktiken
IT-Grundschutzhandbuch 2006	X	X
ITSEC		X
ISO/IEC 13335-1:2004	X	X
ISO 15408 (Common Criteria 2.3)		X
Common Criteria 3.1		X
ISO/IEC 17799:2005, 27002:2005	X	
ISO/IEC 27001:2005	X	
Dr.-Ing. Müller	X	

4.8 Sicherheit im Lebenszyklus

Ziel der Sicherheit ist die Sicherheit des Betriebs einer Anwendung oder eines Computersystems. Doch genau so, wie ein Produkt durch eine abschließende Qualitätskontrolle keine bessere Qualität erhält, verhält es sich auch mit der Sicherheit. Betrachten wir ein Beispiel: Kaum jemand käme bei einem Auto auf die Idee, Überlegungen zum Insassenschutz, z. B. in Form von Airbags oder der Knautschzone, anzustellen, nachdem das Auto gefertigt und eingesetzt worden ist. Dies muss bereits zum Zeitpunkt der Idee für das neue Modell erfolgen und in den folgenden Entwicklungs- und Fertigungsschritten weiter berücksichtigt werden.

Um einen sicheren ITK-Betrieb zu erreichen, genügt es dementsprechend nicht, nur den Betrieb als solches abzusichern und erst in der Betriebsphase Überlegungen zur Sicherheit und Kontinuität anzustellen bzw. Sicherheits- und Kontinuitätsmaßnahmen zu ergreifen. Sicherheit und Kontinuität müssen in den gesamten Lebenszyklus eines jeden Prozesses und jeder Ressource, jedes Produktes und jeder Dienstleistung von der Idee über Konzeption, Entwicklung und Betrieb bis hin zur Außerbetriebnahme verankert werden [6]. Dies betrifft auch begleitende Managementdisziplinen, wie z. B. das Änderungs-, Konfigurations- und Kontinuitätsmanagement.

Betriebssicherheit im Sinne von Ordnungsmäßigkeit sowie Schutz vor menschlichem und technischem Versagen und vor Naturgewalten und Katastrophen ist im gesamten Lebenszyklus zu berücksichtigen. Unter Ordnungsmäßigkeit verstehe ich hierbei Konformität zu gesetzlichen, aufsichtsbehördlichen, vertraglichen und normativen

Voraussetzungen für den sicheren ITK-Betrieb

Betriebs-sicherheit

<i>Angriffs- sicherheit</i>	Vorgaben, Richtigkeit, Aktualität, Vollständigkeit, Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit, Nachvollziehbarkeit und Nachweisbarkeit sowie Verlässlichkeit von Daten und Informationen, ferner Robustheit, Fehlerfreiheit und Zuverlässigkeit von Systemen. Höchstverfügbarkeit im Betrieb beispielsweise erfordert eine geeignete – meist redundante – System- und Infrastrukturarchitektur, die von Anfang an mit zu berücksichtigen ist. Ähnlich verhält es sich mit der Angriffssicherheit, d. h. dem Schutz gegenüber Angriffen und kriminellen Handlungen. Auch hier müssen frühzeitig Maßnahmen ergriffen werden. Denn was nützt die beste Absicherung, wenn in einer Anwendung unzulässiger Programmcode enthalten ist, mit Hilfe dessen sich beispielsweise ein Programmierer Rundungsbeträge bei Zinsgutschriften auf sein eigenes Konto bucht oder nach seinem Ausscheiden aus dem Unternehmen das Programm über eine Hintertür beeinflusst.
<i>Lebenszyklus- und prozess- immanente Sicherheit</i>	Die Integration von Sicherheitselementen in den Lebenszyklus von Prozessen einschließlich der begleitenden Managementdisziplinen bzw. Begleitprozesse sowie Ressourcen führt zu lebenszyklus- und prozessimmanenter Sicherheit [9].

4.9 Ressourcen, Schutzobjekte und -subjekte sowie -klassen

<i>Ressourcen und Schutzobjekte</i>	Prozesse nutzen Ressourcen. Eine Störung, Kompromittierung oder ein Ausfall dieser Ressourcen kann die ordnungsmäßige Funktionsfähigkeit der Geschäftsprozesse beeinträchtigen oder sie komplett ausfallen lassen. Die Ressourcen stellen daher Schutzobjekte dar, die anforderungsgerecht abgesichert werden müssen. Schutzobjekte sind beispielsweise die vom Geschäftsprozess G genutzten Räume R1, R2 und R3 sowie die Informationssysteme I3 und I9. Die konkreten Schutzobjekte – in der objektorientierten Terminologie würden wir von Instanzen reden – können zur einfacheren Handhabung in Schutzobjektklassen zusammengefasst werden.
<i>Schutzsubjekte</i>	Um Unternehmenswerte, d. h. Schutzobjekte, abzusichern, werden ebenfalls Ressourcen eingesetzt. Diese erstrecken sich u. a. von Identitäts- und Rechteverwaltungs- sowie -steuerungssystemen, Firewalls, Virenschnellern und Spamfiltern über Zufahrts- und Zutrittskontrollsysteme, Videoüberwachungs-, Gefahrenmelde- und Netzersatzanlagen sowie unterbrechungsfreie Stromversorgungen bis hin zu Wachdiensten. Diese schützenden Ressourcen und Schutzeinrichtungen sind dementsprechend Schutzsubjekte.

Auch diese Schutzsubjekte müssen geschützt werden, z. B. gegen Ausfall oder Manipulation. Somit sind die Schutzsubjekte gleichzeitig Schutzobjekte, die es ebenfalls abzusichern gilt. So schließt sich der Kreis.

*Schutzsubjekte
und
-objekte*

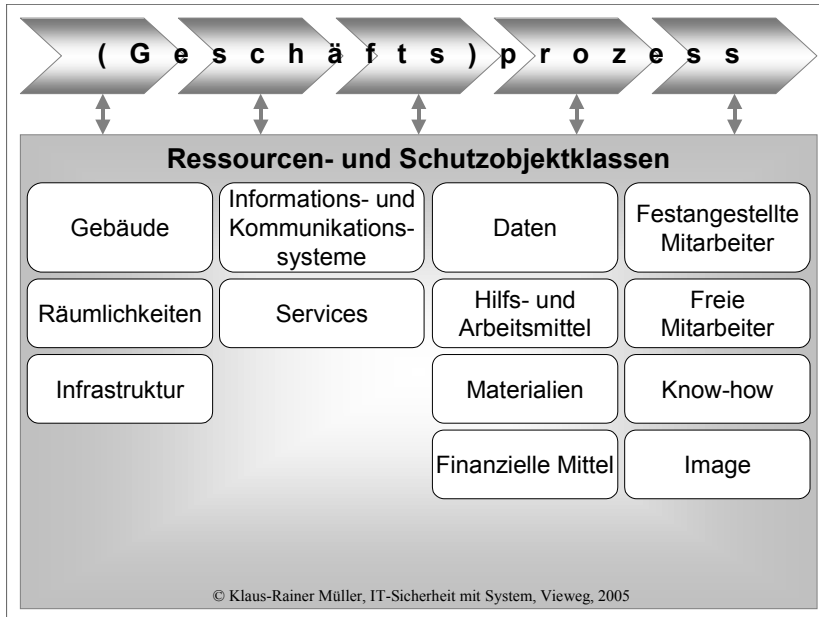


Abb. 4.4: Schutzobjektklassen

Schutzobjekte und -subjekte, d. h. Ressourcen, lassen sich in Klassen zusammenfassen, die üblicherweise durch ähnliche Sicherheitsmaßnahmen geschützt werden können. Dies vereinfacht und standardisiert das Repertoire an Sicherheitsmaßnahmen. Zu den Schutzobjektklassen gehören z. B. Gebäude und Räumlichkeiten einschließlich räumlicher und haustechnischer Infrastruktur, Informations- und Kommunikationssysteme, Daten, Hilfs- und Arbeitsmittel, Anlagen, Materialien, finanzielle Mittel, Prozesse, Services, Know-how und – „last but not least“ – Menschen.

*Klassen,
Schutzobjekt-
klassen*

4.10 Sicherheitskriterien

Um Sicherheit näher zu charakterisieren, gibt es Sicherheitskriterien. Das vorliegende Buch unterscheidet zwischen primären und sekundären Sicherheitskriterien. Zu den primären Sicherheitskriterien zähle ich Konformität (compliance), Robustheit, Verfügbarkeit, Vertrau-

lichkeit, Integrität, Verbindlichkeit und Authentizität. Als sekundäre Sicherheitskriterien sehe ich Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit an.

4.11 Geschäftseinflussanalyse (Business Impact Analysis)

Geschäftseinflussanalysen (Business Impact Analysis {BIA}) bzw. Schutzbedarfsanalysen dienen dazu, die Sicherheitsanforderungen zu ermitteln. Sie werden je Sicherheitskriterium anhand von Schadensszenarien erhoben.

4.12 Geschäftskontinuität (Business Continuity)

Entscheidend für Unternehmen ist die jederzeitige ausreichende Handlungsfähigkeit sowie die Existenzsicherung. Dies bedeutet, dass das Unternehmen die geforderte Verfügbarkeit der Geschäftsprozesse mittels Geschäftseinflussanalysen (Business Impact Analysis) erheben und anschließend deren Einhaltung sicherstellen muss.

*Business
Continuity
Management*

Das Management der Geschäftskontinuität (Business Continuity Management {BCM}) hat hierbei die Aufgabe, die geforderte Verfügbarkeit der Geschäftsprozesse so zu erreichen, dass trotz eines Notfalls oder einer Katastrophe eine angemessene Handlungsfähigkeit des Unternehmens erhalten bleibt. Doch für welche Notfall- und Katastrophenszenarien gilt dies? Ist der zusätzliche Ausfall eines Ausweichstandorts oder gar ein atomarer GAU ebenfalls abzusichern? Und schließlich, mit welcher Risikostrategie soll diese Absicherung erfolgen?

Diese Fragen beantwortet die oberste Ebene der Sicherheitspyramide, die Sicherheits-, Kontinuitäts- und Risikopolitik, mit ihren Aussagen zu den Mindestszenarien und der Risikostrategie. Sie spielt also auch für das Business Continuity Management eine wesentliche Rolle. Die Sicherheitsziele bzw. -anforderungen aus der Business Impact Analysis, der zweiten Ebene der Sicherheitspyramide, fließen ebenfalls in das BCM ein. Auch die folgenden Pyramidenebenen der Transformation zur Umsetzung der Anforderungen sowie der Architektur mit den verfügbaren Sicherheitselementen und deren Struktur finden im BCM Anwendung. Die Ebene der Sicherheitsrichtlinien schließlich stellt beispielsweise standardisierte Gliederungsstrukturen für Notfall- und Katastrophenvorsorgepläne (Business Continuity Plan {BCP}) bereit, die in konkrete Notfall- und Katastrophenpläne münden und zum Schluss getestet, trainiert, umgesetzt und geübt werden.

Dies zeigt, dass BCM keine autarke Insellösung, sondern integraler Bestandteil des Sicherheitsmanagements ist. Doch reicht die Betrachtung der Verfügbarkeit oder gar nur von Ausfällen, um Geschäftskontinuität zu erreichen?

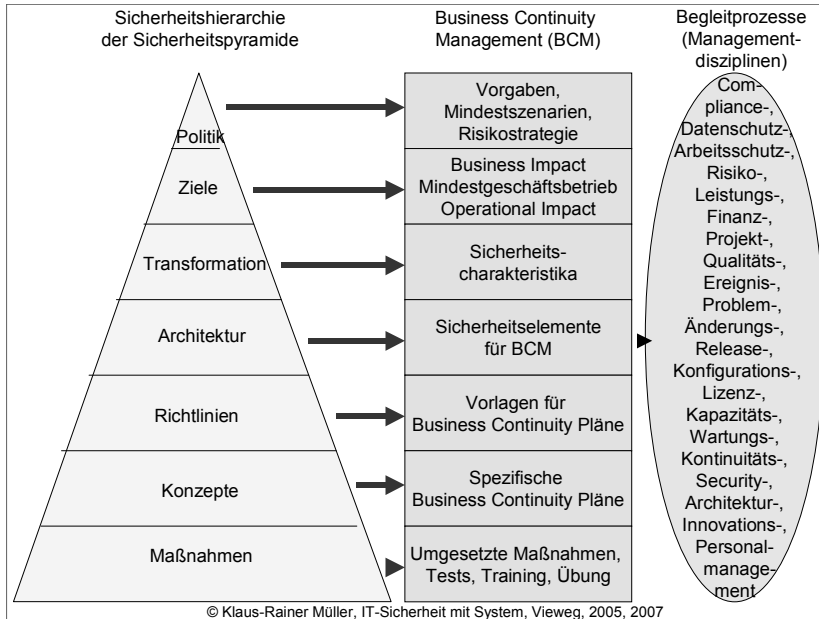


Abb. 4.5: Business Continuity Management mit der Sicherheitspyramide

Bei einer ganzheitlichen Betrachtungsweise ist erkennbar, dass Geschäftskontinuität mehr umfasst als nur primär Ausfälle von Ressourcen, nämlich auch den Schutz vor Angriffen, kriminellen Handlungen, menschlichem Versagen, Fehlverhalten, etc. Alle diese Bedrohungen können letztlich zu einer Einschränkung oder Störung einzelner oder mehrerer Geschäftsprozesse und des regulären Geschäftsbetriebs bis hin zur Handlungsunfähigkeit des Unternehmens führen. So können Erpressung, entwendete oder manipulierte Daten oder Systeme die Ordnungsmäßigkeit und Handlungsfähigkeit beeinträchtigen. Auch sie erfordern dementsprechend Notfallpläne. Somit umfasst das Management der Geschäftskontinuität alle primären und sekundären Sicherheitskriterien von Konformität (compliance) über Robustheit, Verfügbarkeit, Integrität, Vertraulichkeit, Verbindlichkeit und Authentizität bis hin zu Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit.

Sicherheitspyramide für ganzheitliches Business Continuity Management

Damit entspräche das Management der Geschäftskontinuität (Business Continuity Management) jedoch dem unternehmensweiten Sicherheits- und Risikomanagement. Dementsprechend ist die Sicherheitspyramide des Autors ein Vorgehensmodell zum Aufbau eines – wie er es nennt – ganzheitlichen Business Continuity Managements. Der in diesem Buch verwendete Begriff Sicherheitsmanagement ist damit synonym zu ganzheitlichem Business Continuity Management (holistic Business Continuity Management {hBCM}). Dennoch taucht an verschiedenen Stellen des Buchs zusätzlich zum Begriff Sicherheit, der verschiedentlich nur mit Integrität, Vertraulichkeit und Authentizität assoziiert wird, der Begriff Kontinuität auf. In diesen Fällen möchte der Autor noch einmal explizit in Erinnerung rufen, dass auch das Thema Kontinuität mit enthalten ist.

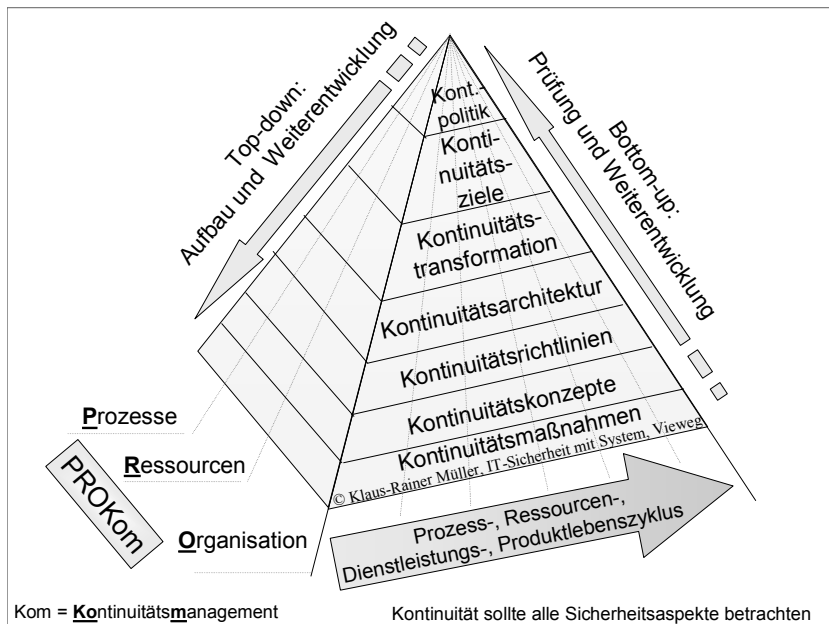


Abb. 4.6 Kontinuitätspyramide IV nach Dr.-Ing. Müller bzw. Kontinuitätsmanagementpyramide nach Dr.-Ing. Müller

Wer sich mit dem Business Continuity Management ausschließlich unter dem Teilaspekt Verfügbarkeit beschäftigen möchte, der kann das Pyramidenmodell bzw. die Sicherheitspyramide des Autors nach wie vor verwenden. Da das Sicherheitskriterium Verfügbarkeit ein Teil der Sicherheitspyramide ist, kann er sie unter diesem Aspekt einsetzen ebenso wie das vorliegende Buch. Die Struktur der Pyra-

mide bleibt dabei gleich. Sie heißt dann jedoch BCM-/Business-Continuity-Management- bzw. Kontinuitäts- oder Kontinuitätsmanagementpyramide (BCM pyramid) nach Dr.-Ing. Müller. Trotz dieser Möglichkeit empfehle ich, für das BCM entweder die Sicherheitspyramide mit allen Sicherheitsaspekten zu verwenden oder die Sicherheitsaspekte unter der Überschrift BCM-Pyramide laufen zu lassen. Grund für meine Empfehlung ist, dass die Verantwortlichen auch im Notfall sicherstellen müssen, dass die Prozesse und Ressourcen die anderen Sicherheitsaspekte nach wie vor angemessen einhalten.

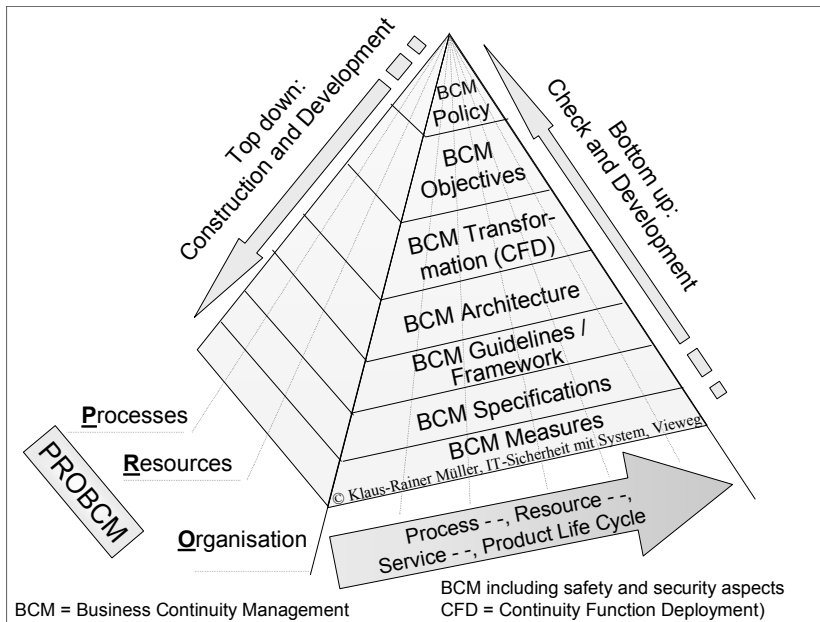


Abb. 4.7 Business Continuity Pyramid IV according to Dr.-Ing. Müller or BCM pyramid IV according to Dr.-Ing. Müller

Im Folgenden nutze ich den Begriff Kontinuitäts- und Business Continuity Management jedoch dem derzeitigen häufigen Sprachgebrauch entsprechend nur für den Teilaspekt Verfügbarkeit.

Kontinuitätsmanagement

4.13 Sicherheit und Sicherheitsdreiklang

Sicherheit ergibt sich aus der Absicherung schützenswerter Werte bzw. Schutzobjekte gegen die potenzielle Möglichkeit, dass eine Bedrohung eine oder mehrere Schwachstellen ausnutzt und so ein ma-

terieller oder immaterieller Schaden entsteht. Sicherheit wird in diesem Buch nicht als „statisch“ und „absolut“ betrachtet, sondern kann – wie auch ein Risiko – Werte annehmen. Sicherheit entspricht somit dem jeweiligen Sicherheitsniveau.

Sicherheit setzt sich zusammen aus dem vorhandenen und zu schützenden Wertniveau, dem durch Sicherheitsmaßnahmen erreichten Schutzniveau sowie dem Bedrohungspotenzial. Dies bezeichne ich als „Sicherheitsdreiklang“.

*Kategorisierung
der Sicherheit*

Sicherheit kann nach unterschiedlichen Themenfeldern kategorisiert werden beispielsweise in Sicherheit gegenüber Verlusten oder Schäden und die Sicherheit, Chancen wahrnehmen zu können. Weitere Unterteilungen sind möglich in

- die Betriebssicherheit, d. h. die Ordnungsmäßigkeit und Sicherheit gegenüber (unbeabsichtigtem) menschlichem und technischem Versagen sowie gegenüber Naturgewalten, wie z. B. Erd- bzw. Seebeben, Stürmen und Überschwemmungen, sowie
- die Angriffssicherheit, d. h. die Sicherheit gegenüber (beabsichtigtem) Fehlverhalten, z. B. in Form von kriminellen Handlungen und Hacker-Angriffen.

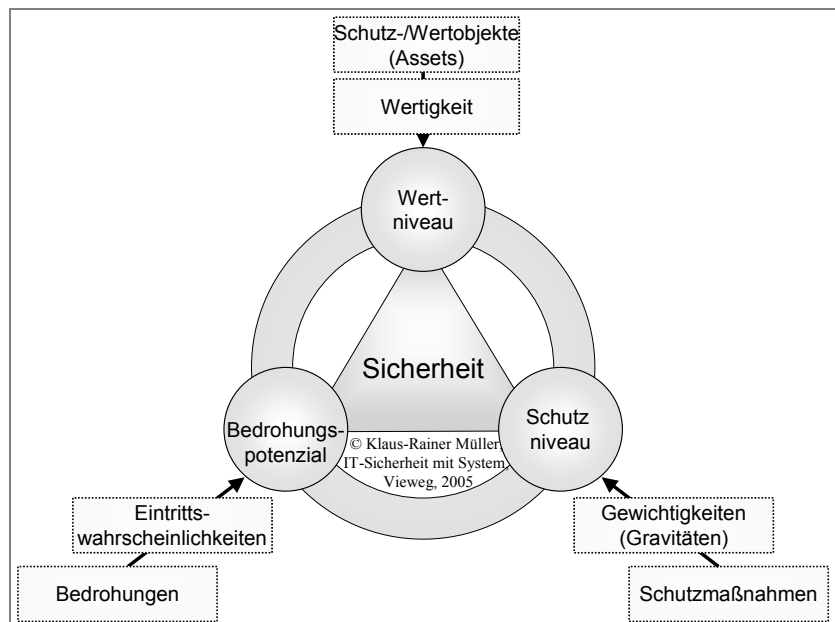


Abb. 4.8 Detaillierter Sicherheitsdreiklang nach Dr.-Ing. Müller

4.14 Risiko und Risikodreiklang

Für den Begriff „Risiko“ finden sich in der Literatur unterschiedliche Definitionen. Zwei gängige sind im Folgenden formuliert.

Die erste Definition lautet: Ein Risiko ergibt sich aus der potenziellen Schadenshöhe multipliziert mit deren Eintrittswahrscheinlichkeit [17] aufgrund einer latent vorhandenen Bedrohung. Diese Sichtweise gewichtet die Auswirkungen eines Schadensereignisses. Sie wird als Brutto-Risiko bezeichnet, weil sie die Wirkung getroffener Sicherheitsmaßnahmen nicht berücksichtigt.

Brutto-Risiko

Das Brutto-Risiko ermöglicht die Priorisierung zu treffender Schutzmaßnahmen. Hierbei ist zu beachten, dass eine Bedrohung trotz einer sehr geringen Eintrittswahrscheinlichkeit dennoch sehr kurzfristig auftreten kann, d. h. morgen, in den nächsten Stunden oder auch im nächsten Augenblick.

Ebenfalls zu berücksichtigen ist, dass Eintrittswahrscheinlichkeiten oftmals retrospektiv sind. D. h. sie basieren auf der Häufigkeit eines Ereignisses in der Vergangenheit. Dementsprechend können derartige Eintrittswahrscheinlichkeiten mehr oder weniger häufigen Veränderungen unterliegen. Beispielsweise können Klimaveränderungen zu häufigeren und stärkeren Stürmen, Schnee- oder Regenfällen und Überschwemmungen, aber auch höheren sommerlichen Außentemperaturen führen, als sie in der Vergangenheit beobachtet wurden. So entstehen Situationen, für die Ressourcen nicht immer ausreichend dimensioniert sind.

Die zweite Definition des Risikos, die in diesem Buch zugrunde gelegt wird, kann demgegenüber als Definition des Netto-Risikos bezeichnet werden. Sie lautet: Ein Risiko ergibt sich aus der potenziellen Möglichkeit, dass eine Bedrohung die Schwachstelle(n) eines oder mehrerer schutzbedürftiger Wertobjekte (Assets) bzw. Schutzobjekte ausnutzt, sodass ein materieller oder immaterieller Schaden entsteht. Diesen Zusammenhang stellt der „Detaillierte Risikodreiklang“ des Autors dar, der in der Abbildung wiedergegeben ist.

Netto-Risiko

Um zu kennzeichnen, dass die Bedrohungen zwar latent vorhanden, aber noch nicht eingetreten sind, wird das Ergebnis aus Bedrohung und Eintrittswahrscheinlichkeit als Bedrohungspotenzial bezeichnet. Aus dem gleichen Grund heißt es Schadens- und Schwachstellenpotenzial.

Der Wert des Netto-Risikos ergibt sich als Brutto-Risiko, d. h. der potenziellen Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit einer latent vorhandenen Bedrohung, multipliziert mit

dem Schwachstellenpotenzial. Das Brutto-Risiko fußt auf dem Schwachstellenpotenzial 100 %, d.h. es wurden keine Sicherheitsmaßnahmen ergriffen, um Schwachstellen zu reduzieren.

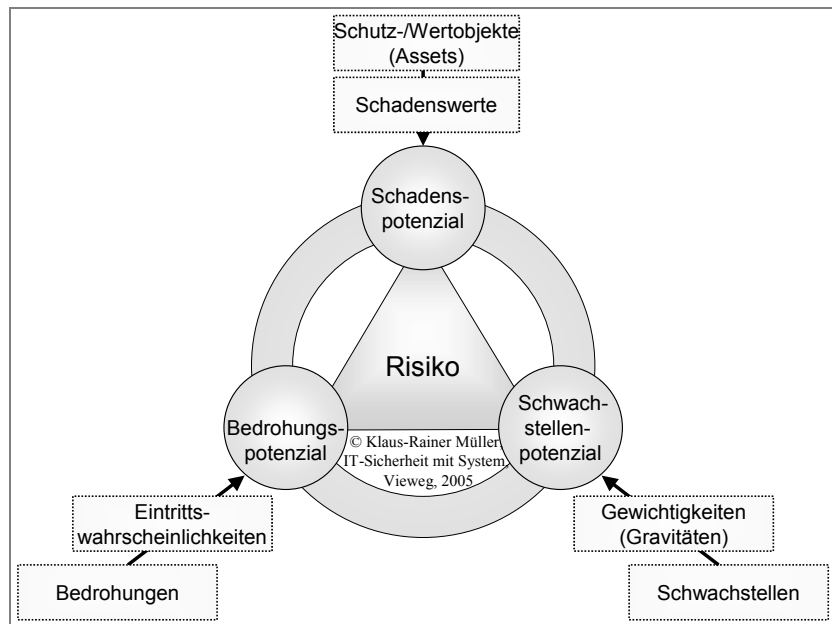


Abb. 4.9: Detaillierter Risikodreiklang nach Dr.-Ing. Müller

Kategorisierung von Risiken

Risiken lassen sich darüber hinaus nach ihren unterschiedlichen Auswirkungen unterscheiden in solche, die einen Schaden oder Verlust bewirken und solchen, die die Wahrnehmung von Chancen verhindern.

Weitere Unterteilungen sind möglich in

- Betriebsrisiken, die durch (unbeabsichtigtes) menschliches und technisches Versagen entstehen
- Naturgewaltenrisiken (Risiken durch Naturgewalten), wie Erd- bzw. Seebeben, Stürme und Überschwemmungen, sowie
- Angriffsrisiken, die durch (beabsichtigtes) Fehlverhalten, z. B. in Form krimineller Handlungen und Hacker-Angriffe, entstehen.

Operationelle Risiken

Die überarbeitete Rahmenvereinbarung „Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen“ [18], kurz Basel II, unterscheidet bei Banken zwischen den Risikokategorien Kreditrisiko, Marktrisiko und Operationelles Risiko.

Welcher Zusammenhang besteht nun zwischen Risiko und Sicherheit? Beide Begriffe charakterisieren zwei unterschiedliche Blickwinkel auf die gleichen Objekte, ähnlich wie ein Glas als halb voll oder halb leer bezeichnet werden kann.

4.15 Risikomanagement

Das Risikomanagement umfasst den Prozess der Erhebung (Risikoinventur), Analyse, Bewertung, Verfolgung, Steuerung und Kommunikation vorhandener Risiken. Steuerung beinhaltet hierbei Maßnahmen zur Ausrichtung des Risikomanagements in Form der Risikopolitik sowie zur Vermeidung (Prevention/Avoidance), Verringerung (Reduction), Verlagerung (Transfer) oder Vereinnahmung (Collection/Acceptance) von Risiken. Der Autor bezeichnet dies als die Müllerschen vier Vs (4Vs) bzw. das Müllersche V-Quadrupel des Risikomanagements oder auch das Risiko-V-Quadrupel. Die englische Abkürzung lautet dann PRTC oder ARTA.

4.16 Zusammenfassung

Das Sicherheits-, Kontinuitäts- und Risikomanagement erstreckt sich über das gesamte Unternehmen und reicht vom Aufbau über die Prüfung und Steuerung bis hin zur Weiterentwicklung. Wesentliches Element ist die frühzeitige Integration der Sicherheit und Kontinuität sowie der Risikobetrachtung in den Lebenszyklus von Prozessen, Ressourcen (z. B. Anlagen und ITK-Systemen), Produkten und Dienstleistungen, um Nachbesserungen, Sicherheitslücken und Risiken möglichst proaktiv zu vermeiden.

Ingenieurmäßige Sicherheit erfordert eine systematische Vorgehensweise, Methodennutzung und Praxisorientierung. Dies bietet die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller.

Die Gegenüberstellung verschiedener Definitionen zeigte, dass der Begriff Sicherheitspolitik unterschiedlich gebraucht wird und von überblicksartigen Unternehmens- bzw. Managementvorgaben bis hin zu spezifischen Regeln und Praktiken reicht. In diesem Buch wird er im Sinne von Unternehmens- bzw. Managementvorgaben verwendet, während übergreifende Regeln und Praktiken als Sicherheitsrichtlinien bezeichnet werden.

Um einen sicheren ITK-Betrieb zu erreichen, muss Sicherheit in den gesamten Lebenszyklus eines Prozesses, einer Ressource, z. B. eines Systems oder einer Anwendung, sowie eines Produktes oder einer Dienstleistung von der Idee über die Konzeption, die Entwicklung

*Sicherheits-,
Kontinuitäts-
und Risiko-
management,
Sicherheit im
Lebenszyklus*

*Ingenieur-
mäßige
Sicherheit*

*Sicherheits-
politik*

Lebenszyklus

und den Betrieb bis hin zur Außerbetriebnahme verankert werden [6]. Dies betrifft auch begleitende Managementdisziplinen, wie z. B. das Änderungs-, Konfigurations-, Beschwerde- und Kontinuitätsmanagement.

*Ressourcen,
Schutzobjekte
und
-subjekte sowie
Schutzobjekt-
klassen*

Prozesse nutzen Ressourcen, die auch als Schutzobjekte bezeichnet werden. Zu ihrem Schutz werden Ressourcen eingesetzt, wie z. B. Firewalls und Virens Scanner, die der Autor als Schutzsubjekte bezeichnet. Die Schutzobjekte, aber auch Schutzsubjekte, müssen gemäß den Anforderungen der Geschäftsprozesse abgesichert werden. Ressourcen und so auch Schutzobjekte können in Klassen zusammengefasst werden. Zu den Schutzobjektklassen gehören Menschen, Gebäude, Räumlichkeiten, haustechnische Infrastruktur, Informations- und Kommunikationssysteme, Daten, Arbeitsmittel, finanzielle Mittel, Prozesse, Services und Know-how.

*Sicherheits-
kriterien*

Der Oberbegriff Sicherheit wird konkretisiert durch die primären Sicherheitskriterien Konformität (compliance), Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie die sekundären Sicherheitskriterien Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit.

*Geschäftsein-
flussanalyse*

Geschäftseinflussanalysen (Business Impact Analysis {BIA}) bzw. Schutzbedarfsanalysen dienen dazu, die Sicherheitsanforderungen zu ermitteln.

*Risiko und
Sicherheit*

Der Begriff Risiko kann als Brutto- oder Netto-Risiko betrachtet werden. Das Brutto-Risiko ergibt sich aus der potenziellen Schadenshöhe multipliziert mit der Eintrittswahrscheinlichkeit einer latent vorhandenen Bedrohung. Das Netto-Risiko ergibt sich daraus, dass das tatsächlich vorhandene Schwachstellenpotenzial mit berücksichtigt wird. Dazu wird das im Brutto-Risiko als 100 % angenommene Schwachstellenpotenzial um ergriffene Sicherheitsmaßnahmen reduziert. Das Netto-Risiko besteht dementsprechend aus Schadens-, Bedrohungs- und Schwachstellenpotenzial. Der detaillierte Risikodreiklang des Autors veranschaulicht die Zusammenhänge.



Die Begriffe Risiko und Sicherheit stellen zwei Seiten derselben Medaille dar, ähnlich wie ein Glas als halb voll oder halb leer bezeichnet werden kann.

5 Die Sicherheitspyramide – Strategie und Vorgehensmodell

Vorhandene Sicherheitskonzepte und -maßnahmen sind oft Insellösungen oder Ad-hoc-Maßnahmen mit unterschiedlichem Sicherheitsniveau. Hieraus ergibt sich eine latente Bedrohung für die Handlungsfähigkeit und das Image eines Unternehmens. Hinzu kommen oftmals hohe Abhängigkeiten vom Know-how einzelner Mitarbeiter.

Insellösungen

Ursache von Sicherheitsdefiziten ist des Öfteren einerseits die Unkenntnis der Anforderungen und andererseits die zu späte Berücksichtigung dieser Anforderungen im Lebenszyklus eines Prozesses, einer Ressource, eines Produktes oder einer Dienstleistung. Fragen danach, wie umfänglich Sicherheitsmaßnahmen sein sollen oder was sie wie stark und wogegen schützen sollen, können häufig nicht beantwortet werden.

Sicherheitsdefizite

Die Sicherheitspyramide oder genauer, die Sicherheitsmanagementpyramide des Autors bietet ein strukturiertes, strategisches und praxisorientiertes Top-down-Vorgehensmodell zum ganzheitlichen Aufbau und zur Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements. Durch die Berücksichtigung des Lebenszyklus von Prozessen, Ressourcen, Dienstleistungen und Produkten kann eine prozess-, ressourcen-, leistungs- und produkt- sowie lebenszyklusimmanente Sicherheit erreicht werden.

Sicherheitspyramide

Die folgenden Unterkapitel behandeln die Themen:

1. Überblick über die Sicherheitspyramide
2. Sicherheitshierarchie
3. PROSim (Prozesse, Ressourcen und Organisation für das Sicherheitsmanagement)
4. Prozess-, Ressourcen-, Leistungs- und Produktlebenszyklus
5. Sicherheitsregelkreis für den Aufbau, die Steuerung und die Weiterentwicklung des Sicherheitsmanagements
6. Sicherheitsmanagementprozess
7. Zusammenfassung

5.1 Überblick

Die Sicherheitspyramide IV, kurz SiPyr IV genannt, basiert auf dem Allgemeinen Pyramidenmodell IV des Autors. Sie besteht aus 7 Ebenen, hat 3 Dimensionen, beinhaltet einen Regelkreis und einen Sicherheitsmanagementprozess. Die Sicherheitspyramide stellt ein anschauliches, durchgängiges, ganzheitliches und systematisches Vorgehensmodell für den Aufbau und die Weiterentwicklung eines prozess-, ressourcen-, leistungs-, produkt- und lebenszyklusimmanenten Sicherheits-, Kontinuitäts- und Risikomanagements dar. Hierzu verbindet sie den hierarchischen Aufbau mit Prozessen, Ressourcen und Organisation sowie den Lebenszyklen von Prozessen, Ressourcen, Produkten und Dienstleistungen. Die Sicherheitspyramide des Autors integriert seit langem Themenbereiche und Aspekte, die in unterschiedlichem Umfang und Detaillierungsgrad sowie als Teilperspektiven in Normen, Standards und Practices vorkommen bzw. inzwischen aufgenommen wurden.

Bestehende Normen, Standards, Good und Best Practices zum Thema Sicherheit und Sicherheitsmanagement unterscheiden sich im Vorgehensmodell, der Ganzheitlichkeit, Detaillierungstiefe und den betrachteten Sicherheitsdimensionen (z. B. Hierarchie, Prozesse, Lebenszyklus). Sie haben unterschiedliche Schwerpunkte und fokussieren sich primär auf einzelne Themenbereiche. Insbesondere die ISO-Normen bewegen sich dabei häufig auf einem überblicksartigen Niveau. Die folgenden Normen, Standards und Practices behandeln schwerpunktmäßig u. a. folgende Themen:

- die ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management: einen möglichen hierarchischen Aufbau des Sicherheitsmanagements im Unternehmen sowie eine übergreifende Organisation
- die ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management: die Risikobewertung und -behandlung, das Management der Unternehmenswerte, die Sicherheitspolitik, die organisatorische, personelle und physische Sicherheit, das Management des Betriebs, IT-sicherheitsrelevanter Ereignisse und der Geschäftskontinuität, die Zugangskontrolle, die Beschaffung, Entwicklung und Wartung von IT-Systemen sowie die Compliance
- die ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements:

den Sicherheitsmanagementprozess auf Basis des PDCA-Zyklus (Plan-Do-Check-Act) sowie die Themen Begriffe und Definitionen, Informationssicherheitsmanagementsysteme (ISMS), Verantwortung des Managements, internes ISMS Audit, Management Review des ISMS, Verbesserung des ISMS, Kontrollziele und Kontrollen, OECD-Prinzipien und der Standard ISO/IEC 27001:2005

- das IT-Grundschutzhandbuch des BSI, Stand 2006: eine Vorgehensweise für den IT-Sicherheitsprozess und für den Aufbau des IT-Sicherheitsmanagements sowie sehr umfangreiche IT-Grundschutzkataloge mit Gefährdungs- und Maßnahmenkatalogen. Die IT-Grundschutzkataloge enthalten seit Ende 2005 einen Lebenszyklus der dortigen Bausteine. Seit November 2006 ist in der Maßnahme M 2.338 ein rudimentärer hierarchischer Aufbau aus drei Ebenen mit Unterebenen in Dreiecksform dargestellt. Ebenfalls Ende 2006 hinzugekommen ist die Maßnahme „System-Entwicklung“ (M 2.378) mit lebenszyklusorientierten Ausführungen, die sich angabegemäß am V-Modell sowie teilweise an den Vorgaben der ITSEC/CC orientieren. In der Nomenklatur der Sicherheitspyramide handelt es sich um den Lebenszyklus eines IT-Systems
- der BS 25999-1:2006: das Business Continuity Management
- die ISO/IEC 15408, die auf den Common Criteria 2.1 basiert: den Lebenszyklus von IT-Evaluationsgegenständen
- die Best Practices nach ITIL®: die verschiedenen IT-Prozesse, sowie in der Version 3 ab 2007 den IT Service Lifecycle
- die ISO 20000: die verschiedenen IT-Prozesse
- das COBIT®-Framework: die Informationskriterien, die IT-Ressourcen und die IT-Prozesse sowie Kontrollelemente.

Die Sicherheitspyramide IV des Autors beinhaltet das durchgängige Vorgehensmodell für das Sicherheits-, Kontinuitäts- und Risiko- sowie Compliancemanagement. Sie enthält die hierarchische Struktur, die Prozesse, die Ressourcen und die Organisation, die Lebenszyklen und schließlich den Sicherheits- und Kontinuitätsmanagementprozess sowie den Controlling-Prozess in Form des Sicherheitsregelkreises. Der Autor stellte die Sicherheitspyramide 1995 auf den Datensicherheitstagen [1] erstmals einem breiteren Publikum vor. Die weiterentwickelte zweite Version veröffentlichte der Autor 1996 in der Zeitschrift KES [5]. Hier wie auch in verschiedenen Artikeln [6], [7] sowie im Buch „IT-Sicherheit mit System“ [4], in dem der Autor die Sicherheitspyramide erstmals dreidimensional dargestellt hat, wies er darauf hin, dass der gesamte Prozess der Softwareerstellung auch unter Berücksichtigung der Sicherheitskriterien zu betrachten ist. Die drei-

*Historie der
Sicherheits-
pyramide*

dimensionale Sicherheitspyramide lässt sich für die gesamte Palette an Sicherheits-, Kontinuitäts- und Risikothemen eines Unternehmens nutzen.

Die Elemente der Sicherheitspyramide sind ausgerichtet auf die primären Sicherheitskriterien Konformität, Robustheit, Verfügbarkeit und Kontinuität, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie die sekundären Sicherheitskriterien Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit.

Die Sicherheitspyramide veranschaulicht die teilweise komplexen und vielfältigen Zusammenhänge des Sicherheitsmanagements. Sie schafft eine strukturierte Basis zum systematischen Erfassen der Anforderungen und deren Abbildung in Form von Sicherheitsmaßnahmen. So können fehlende Sicherheitselemente erkannt werden.

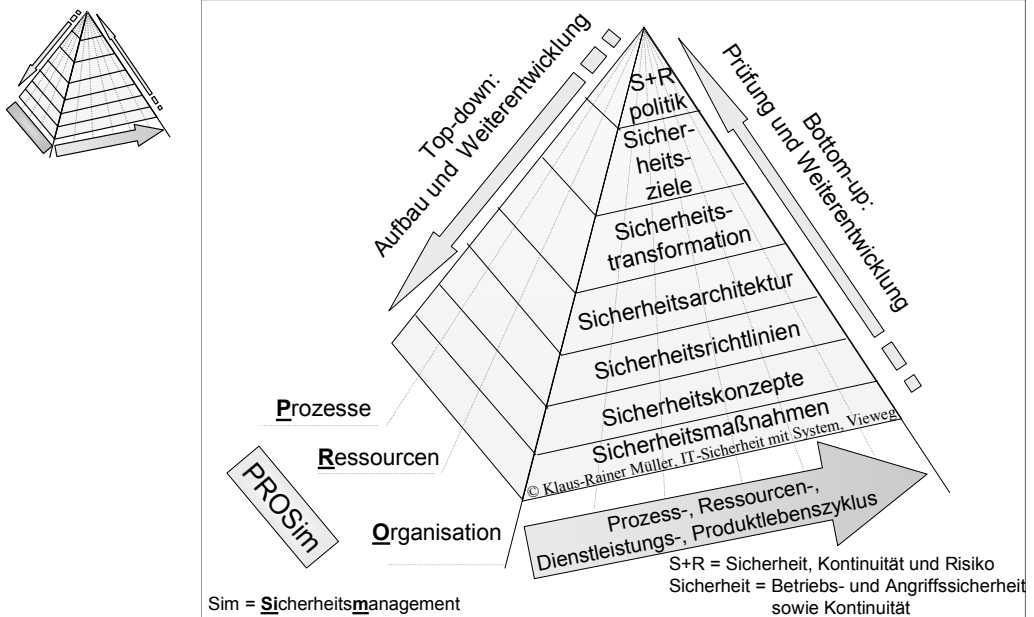


Abb. 5.1: Sicherheitspyramide IV nach Dr.-Ing. Müller bzw. Sicherheitsmanagementpyramide nach Dr.-Ing. Müller

*Sicherheits-
hierarchie*

Die erste Dimension der Sicherheitspyramide ist die Sicherheitshierarchie. Sicherheit ist hierbei im Sinne von Betriebs- und Angriffssicherheit sowie Kontinuität zu verstehen. Die Ebenen der Sicherheitspyramide leiten sich top-down voneinander ab:

- Sicherheits-, Kontinuitäts- und Risikopolitik
- Sicherheitsziele / Sicherheitsanforderungen
- Sicherheitstransformation
- Sicherheitsarchitektur
- Sicherheitsrichtlinien - Generische Sicherheitskonzepte
- Spezielle Sicherheitskonzepte
- Sicherheitsmaßnahmen

Für englischsprachige Unternehmen lauten die entsprechenden Bezeichnungen:

*Safety/
security and
continuity
hierarchy*

- safety/security, continuity and risk policy
- safety/security and continuity objectives / requirements
- safety/security and continuity function deployment
- safety/security and continuity architecture
- safety/security and continuity guidelines
- safety/security and continuity specification
- safety/security and continuity measures (safeguards)

Diese Hierarchieebenen unterteilen sich jeweils in folgende Unter-ebenen:

- Vorbeugung (Prävention),
Pflege,
Übung und
Überprüfung (Verifikation)
- Beobachtung (Monitoring),
Erkennung (Detektion),
Meldung/Alarmierung
- Erwidern (Reaktion), z. B. Abwehr
- Beurteilung (Evaluation) des Schadens
- Wiederherstellung (Restauration)
- Verbesserung (Emendation)

Die zweite Dimension umfasst die folgenden Themenstellungen:

*Prozesse,
Ressourcen und
Organisation*

- Prozesse
- Ressourcen,
z. B. Gebäude, haustechnische Infrastruktur, Anlagen, Systeme
{u. a. ITK-Systeme}, Material, finanzielle Mittel, Methoden, Know-
how, Image, Hilfsmittel und Tools und nicht zuletzt Personal
- Organisation,
die je hierarchischer Ebene im Hinblick auf das Sicherheits-

management zu berücksichtigen sind. Diese Themenstellungen fasse ich unter der Bezeichnung PROSim zusammen.

Im Vergleich zur Bezeichnung ProTOPSi bei der Sicherheitspyramide III sind die Begriffe Technologie und Personal sowie alle weiteren Schutzobjekte zum Oberbegriff Ressource zusammengeführt. Alternativ kann auch die Bezeichnung PROMSim verwendet werden, um „Menschen“ ihrer Bedeutung entsprechend nicht unter Ressourcen, sondern separat einzugruppieren.

<i>Lebenszyklus</i>	Die dritte Dimension behandelt die einzelnen Phasen im Lebenszyklus des jeweiligen Prozesses, der jeweiligen Ressourcen, Produkte oder Dienstleistungen und orientiert sich am zugrunde liegenden Phasenmodell.
<i>Sicherheitsregelkreis, -prozess</i>	Umrahmt wird die Sicherheitspyramide von einem Regelkreis und dem Sicherheitsmanagementprozess, über den der Aufbau, die Prüfung, Steuerung und Weiterentwicklung sowie das Berichtswesen erfolgen.
<i>Gesamtheitliche Struktur</i>	Vor dem Aufbau des Sicherheitsmanagements existieren in Unternehmen oftmals nur fragmentarische Ansätze zum Sicherheitsmanagement. Eine gesamtheitliche Struktur, vollständige Konzepte, Prozessorientierung etc. fehlen.

Wer auf die Sicherheitspyramide übergeht, kann die vorhandenen Sicherheitsbausteine seines Unternehmens nutzen, indem er sie den jeweiligen hierarchischen Ebenen der Sicherheitspyramide zuordnet. Hierbei prüft er, welchen Einfluss diese Bausteine auf die höheren Hierarchieebenen haben. Der IT-Sicherheitsverantwortliche stellt sich beispielsweise die Frage, welche Sicherheitskonzepte für Betriebssysteme sich so abstrahieren und konsolidieren lassen, dass sie in der Folge als betriebssystemübergreifende Sicherheitsrichtlinien zur Verfügung gestellt werden können. Anschließend baut er die Sicherheitspyramide top-down auf, wobei er die im Unternehmen vorhandenen Bausteine zur Sicherheit entsprechend anpasst.

5.2 Sicherheitshierarchie

Die Sicherheitspyramide besitzt einen hierarchischen Aufbau. Dieser ermöglicht es, ausgehend vom Unternehmenszweck und der darin begründeten Sicherheitspolitik, ein strukturiertes und nutzenorientiertes Sicherheits-, Kontinuitäts- und Risikomanagement aufzubauen.

5.2.1 Sicherheits-, Kontinuitäts- und Risikopolitik

Die oberste Ebene, nämlich die Sicherheits-, Kontinuitäts- und Risikopolitik, ist der Ausgangspunkt für den Aufbau der Sicherheitspyramide. In ihr beschreibt das Top Management, abgeleitet von der Unternehmenspolitik, welche Bedeutung Sicherheit und Kontinuität für das Unternehmen haben und welche übergreifenden Ziele es zu erreichen gilt. Zu den übergreifenden Zielen gehören u. a. die Einhaltung von Gesetzen, der Schutz von Personen und Unternehmenswerten. Das Top Management legt dar, welche Risikostrategie das Unternehmen verfolgt. Es stellt sich selbst im Sinne einer Vorbildfunktion an die Spitze des Sicherheits-, Kontinuitäts- und Risikomanagements und verpflichtet sich, die erforderlichen Mittel und Ressourcen bereitzustellen. Die Sicherheits-, Kontinuitäts- und Risikopolitik beschreibt darüber hinaus die prinzipielle Struktur des Sicherheits-, Kontinuitäts- und Risikomanagements im Unternehmen.

5.2.2 Sicherheitsziele / Sicherheitsanforderungen

Ausgehend von der Sicherheits-, Kontinuitäts- und Risikopolitik legen die Verantwortlichen die Sicherheitsziele bzw. -anforderungen je Prozess bzw. Organisationseinheit fest. Hierzu müssen die Produkte und Leistungen sowie die dafür erforderlichen Kerngeschäfts- und Supportprozesse bzw. die Organisationseinheiten und ihre Aufgaben sowie ihr Zusammenspiel bekannt sein. Außerdem muss erhoben worden sein, welche dieser Prozesse bzw. Organisationseinheiten welche Ressourcen, z. B. ITK-Systeme nutzen.

Anhand allgemeiner Szenarien, z. B. Ausfall oder Datenmanipulation, ermitteln die Prozess- oder Ressourcenverantwortlichen die Folgen von Sicherheitsverletzungen und definieren den Schutzbedarf der Prozesse und der von ihnen genutzten ITK-Systeme. Die Prozesse und die Informationssysteme werden in Schutzbedarfsklassen – auch als Sicherheits- oder Kritikalitätsklassen bezeichnet – eingeordnet.

5.2.3 Sicherheitstransformation

Die Sicherheitsziele sind aus Sicht der Geschäftsprozesse formuliert. Beispielsweise besteht die Forderung nach einem Rund-um-die-Uhr-Betrieb für ein Informationssystem. Doch wie lässt sich dies in der ITK realisieren? Hierzu ordnen die IT-Verantwortlichen den Anforderungen der Geschäftsprozesse die Möglichkeiten der ITK zu. Für einen Rund-um-die-Uhr-Betrieb sind u. a. redundante Rechnersysteme, gespiegelte Plattenspeicher, Konzepte zur Katastrophenvorsorge, definierte Prozesse und geschulte Mitarbeiter erforderlich. Es erfolgt somit eine Transformation der Anforderungen aus Nutzersicht auf

die prozessualen, ressourcenspezifischen, technologischen und organisatorischen Möglichkeiten der ITK. Diese Transformation bezeichne ich als Sicherheitstransformation bzw. in Analogie zum Quality Function Deployment (QFD) als Safety, Security and Continuity Function Deployment (SSCFD).

5.2.4 Sicherheitsarchitektur

Die Sicherheitsarchitektur enthält die prinzipiellen Sicherheitsanforderungen und prinzipiellen Bedrohungen sowie die Sicherheitsprinzipien und –strategien. Sie stellt ferner die prinzipiellen Sicherheitselemente auf, mittels derer die Sicherheitsanforderungen und damit das gewünschte Sicherheitsniveau erreicht werden sollen. Die Sicherheitselemente beziehen sich auf die Prozesse, die Ressourcen und die Organisation sowie den Produkt-, Leistungs-, Prozess- und Ressourcenlebenszyklus. Beispiele für den Ressourcenlebenszyklus sind der Software- und ITK-Systemlebenszyklus.

5.2.5 Sicherheitsrichtlinien

Sicherheitsrichtlinien – generische Sicherheitskonzepte

Die Sicherheitsrichtlinien (guidelines), auch als Sicherheitsstandards oder generische Sicherheitskonzepte bezeichnet, beinhalten alle Sicherheitsregeln, -richtlinien und -standards eines Unternehmens. Sie sind sozusagen der übergreifende Know-how-Speicher, den das Unternehmen kontinuierlich überprüft und weiterentwickelt.

Seine Veränderungsgeschwindigkeit ist nicht sehr stark, da hier vorwiegend übergreifende und nicht systemspezifische Elemente enthalten sind. Generische Sicherheitskonzepte sind somit unabhängig von Plattformen, z. B. Rechnerplattformen, Anwendungen etc. Diese übergreifenden Sicherheitsrichtlinien geben die Richtung vor für die anschließende Entwicklung entsprechender plattformspezifischer Konzepte. Sie schaffen die Basis für ein weitgehend einheitliches Sicherheitsniveau, wie es insbesondere auch für Konzerne und international aufgestellte Unternehmen erforderlich ist.

5.2.6 Spezifische Sicherheitskonzepte

Spezifische Sicherheitskonzepte setzen die generischen Sicherheitsregeln, -richtlinien und -standards auf konzeptioneller und system- bzw. plattformspezifischer Ebene um. Hier können sich häufiger Änderungen ergeben, da sich der Markt und somit die angebotenen Systeme kontinuierlich weiterentwickeln. Beispielsweise können sich generische Standards, die sich in einem Betriebssystemrelease nicht realisieren ließen, im nächsten Release umsetzen lassen. Das Betriebs-

system kann dann möglicherweise für Anwendungen eingesetzt werden, die ein höheres Sicherheitsniveau benötigen.

5.2.7 Sicherheitsmaßnahmen

Sicherheitsmaßnahmen stellen die reale und dokumentierte Implementierung der Sicherheitskonzepte in Form konkreter Prozesselemente, Technologien, Verfahren, Mechanismen, Prozeduren, organisatorischer oder personeller Maßnahmen dar. Wurde beispielsweise ein Sicherheitskonzept erstellt, in dem eine Vereinzelungsanlage und deren Eigenschaften vorgeschrieben sind, so stellt die Realisierung dieses Konzepts durch die spezifische Vereinzelungsanlage eines bestimmten Herstellers eine Sicherheitsmaßnahme dar. Eine andere Sicherheitsmaßnahme ist die Implementierung des vorgeschriebenen Zugriffsschutzes mittels eines Zugriffssteuerungssystems durch das Setzen der entsprechenden Parameter.

5.3 PROSim

Zur Etablierung der geforderten Sicherheit sind Sicherheitsmaßnahmen erforderlich, die sich auf die Prozesse, die Ressourcen und die Organisation im Hinblick auf das Sicherheitsmanagement beziehen. Dies bezeichne ich als PROSim.

Der Begriff Prozess umfasst hierbei Kern-, Support- und Begleitprozesse.

Prozesse

Der Begriff Ressource ist bewusst sehr weit gefasst. Hierunter verstehe ich alle materiellen und immateriellen und nicht zuletzt personellen Ressourcen. Sie reichen vom Gebäude mit seinen Räumlichkeiten und der haustechnischen Infrastruktur über Fertigungsstraßen, Produktionsanlagen, Maschinen, Informations- und Kommunikationssysteme, Hilfs- und Arbeitsmittel, Materialien, finanzielle Mittel, Methoden, Daten, Know-how, Image und Services bis hin zu Personal.

Ressourcen

Die Organisation umfasst die Linienorganisation, wie sie beispielsweise im Organigramm mit Geschäfts-, Bereichs-, Abteilungs- und Gruppenleitung sowie Stabsabteilungen dargestellt ist, sowie Rollen, wie z. B. Projektmanager und -leiter.

Organisation

Damit eine ganzheitliche, prozess- und lebenszyklusimmanente Sicherheit entsteht, muss PROSim je Hierarchieebene der Sicherheitspyramide und je Lebenszyklusphase berücksichtigt, beschrieben und integriert werden.

*Prozess- und
lebenszyklus-
immanente
Sicherheit*

5.4 Lebenszyklus von Prozessen, Ressourcen, Produkten und Leistungen (Services)

Sicherheit ebenso wie Qualität ist das Ergebnis von Maßnahmen, die im Vorfeld eingeführt worden sind. Betrachten wir zum Vergleich die Qualitätskontrolle am Ende eines Produktionsprozesses eines Autos. Sie kann letztlich nur feststellen, ob die geforderte Qualität erreicht wurde oder nicht. Veränderungen sind nur noch in Form von Nachbesserungen möglich. Entscheidend ist daher, Qualitätssicherungsmaßnahmen bereits zu einem sehr frühen Zeitpunkt einzuführen. Dies beginnt bei der Ermittlung der Kundenanforderungen, muss in technische Eigenschaften transformiert und bei der Entwicklung berücksichtigt werden. Ebenfalls einzubeziehen sind die Fertigungsmöglichkeiten.

*Lebenszyklus-
immanente
Sicherheit*

Diese Aussagen gelten analog für das Thema Sicherheit. Sicherheitsanforderungen an eine Dienstleistung oder ein Produkt, an die dazu erforderlichen Kern-, Support- und Begleitprozesse sowie die genutzten Ressourcen bzw. ITK-Systeme müssen, beginnend mit dem Zeitpunkt der ersten Idee, sowie in den folgenden Phasen des Lebenszyklus berücksichtigt werden. Dies bezeichne ich als lebenszyklusimmanente Sicherheit.

5.4.1 Geschäfts-, Support- und Begleitprozess-Lebenszyklus

Ein Unternehmen besitzt eine Vielzahl von Kerngeschäftsprozessen und unterstützenden Geschäftsprozessen (Supportprozesse), denen Begleitprozessen zur Seite stehen. Kerngeschäftsprozesse sind dadurch gekennzeichnet, dass sie vom externen Kunden ausgehen und beim externen Kunden enden, d. h. ihr Ergebnis an den externen Kunden liefern. Supportprozesse unterstützen die Kerngeschäftsprozesse, indem in ihnen Teilaufgaben durchgeführt werden. Begleitprozesse bzw. Managementdisziplinen laufen entlang dem Lebenszyklus parallel zu diesen Prozessen. Beispiele hierfür sind das Änderungs-, Konfigurations- und Problemmanagement, aber auch das Kapazitäts-, Kontinuitäts- und Datensicherungsmanagement.

Bei der Gestaltung all dieser Prozesse sind Sicherheitsaspekte zu berücksichtigen. Diese müssen bereits bei der Idee und der Konzeption der Prozesse mit betrachtet werden. Sie finden anschließend ihren Niederschlag in der Test-, Pilotierungs-, Einführungs- und Betriebsphase bis hin zum Zeitpunkt ihrer Außerbetriebnahme. Sicherheit ist also während aller Phasen eines Prozesses, d. h. während des gesamten Lebenszyklus zu berücksichtigen und z. B. durch die Revision zu prüfen.

Ähnlich, wie es beim Qualitätsmanagement an verschiedenen Stellen des jeweiligen Prozesses präventive, begleitende und postventive Qualitätssicherungsmaßnahmen gibt, müssen in die Prozesse sicherheitsrelevante Maßnahmen integriert werden. Dadurch lässt sich eine lebenszyklusimmanente Prozesssicherheit erreichen.

*Lebenszyklus-
immanente
Prozess-
sicherheit*

Sicherheitsmaßnahmen können beispielsweise Funktionstrennungen, die Einführung des Vier-Augen-Prinzips und unterschiedliche Berechtigungsstufen (Vollmachten) sein.

5.4.2 Ressourcen-/Systemlebenszyklus

Alle Ressourcen besitzen einen Lebenszyklus, in dem Sicherheitsaspekte zu berücksichtigen sind. Im Bereich der ITK existiert eine Vielzahl von Vorgehensmodellen für die Entwicklung eines Systems. Handelt es sich um ein Anwendungssystem, bestehend aus Hardware, Software und Dokumentation, so sind häufig Phasenmodelle für die Entwicklung vorhanden.

*Lebenszyklus-
immanente
ITK-System-
sicherheit*

Wer lebenszyklusimmanente ITK-Systemsicherheit erreichen will, muss in diesen Entwicklungsprozess Sicherheitselemente integrieren. Hierdurch lassen sich Sicherheitsprobleme im Betrieb präventiv reduzieren oder vermeiden.

5.4.3 Dienstleistungs- und Produktlebenszyklus

Nicht zuletzt aufgrund des Produkthaftungsgesetzes spielt die Sicherheit von Produkten eine wesentliche Rolle. Aber auch die Erbringung von IT-Dienstleistungen erfordert die Einhaltung gesetzlicher und vertraglicher Sicherheitsanforderungen. Zu Beginn des Lebenszyklus sind daher die Sicherheitsanforderungen Teil der Anforderungsspezifikation. Sie werden über die verschiedenen Entwicklungsschritte weiter verfeinert, umgesetzt und getestet, bevor die Dienstleistung erbracht oder das Produkt verkauft wird.

*Lebenszyklus-
immanente
Dienst-
leistungs- und
Produkt-
sicherheit*

5.5 Sicherheitsregelkreis

Die Sicherheitspyramide bietet eine systematische Vorgehensweise, um das Sicherheits-, Kontinuitäts- und Risikomanagement eines Unternehmens aufzubauen und zu strukturieren. Wäre dies das Ende der Aktivitäten, so ergäbe sich ein „statisches“ Ergebnis. Da sich aber das Erkenntnisniveau und das Umfeld dynamisch ändern, muss sich auch das Sicherheits-, Kontinuitäts- und Risikomanagementsystem kontinuierlich weiterentwickeln. Der Sicherheitspyramide muss daher noch „Leben eingehaucht“ werden.

Dies erfolgt durch einen Steuerungsmechanismus, den Sicherheitsregelkreis. Zu Beginn werden Sicherheitsziele festgelegt, vereinbart und in eine Planung umgesetzt. Den Ist-Zustand verfolgen die Verantwortlichen kontinuierlich. Sie erstellen Prognosen über die Zielerreichung, führen Abweichungsanalysen durch und leiten gegebenenfalls Korrekturmaßnahmen ein. Ein regelmäßiges Berichtswesen schafft Transparenz.

Zu den Elementen im Sicherheitsregelkreis gehören Safety-Security-Prüfungen oder -Audits, die von internen oder externen Sicherheitsauditeuren durchgeführt werden.

5.6 Sicherheitsmanagementprozess

PDCA-Zyklus

Der Sicherheitsmanagementprozess, der den Kontinuitäts- und Risikomanagementprozess beinhaltet bzw. beinhalten kann, leitet sich aus der Sicherheitspyramide des Autors ab. Er orientiert sich am PDCA-Zyklus (Plan-Do-Check-Act) und beschreibt, wie das Sicherheitsmanagement eines Unternehmens geplant, aufgebaut und in die Prozesse und Ressourcen sowie deren Lebenszyklen integriert wird. Der Sicherheitsmanagementprozess schließt die Umsetzung (Do) in Form des Betriebs mit ein, in dem Monitoring und Controlling wichtige Themen sind. Prüfungen (Check) liefern Informationen über den Status des Sicherheitsmanagements. Die letzte Phase der Verbesserung (Act) wertet die Ergebnisse aus. Hieraus ergeben sich Verbesserungsmaßnahmen für den Einstieg in die Planung und den nächsten Durchlauf des PDCA-Zyklus ab.

5.7 Zusammenfassung

*Drei-
dimensionale
Sicherheits-
pyramide*

Die Sicherheitspyramide IV nach Dr.-Ing. Müller ist dreidimensional. Die erste Dimension verläuft vertikal und beinhaltet die hierarchisch aufeinander aufbauenden Ebenen des Sicherheitsmanagements. Die zweite Dimension beschreibt die dazugehörigen Elemente Prozesse, Ressourcen und Organisation für das Sicherheitsmanagement (PRO-Sim). Die dritte Dimension berücksichtigt den Prozess-, Ressourcen-, Dienstleistungs- und Produktlebenszyklus.

*1. Dimension:
Sicherheits-
hierarchie*

Die oberste Ebene und damit den Ausgangspunkt der Sicherheitspyramide IV bilden die geschäftspolitischen Sicherheitsanforderungen des Unternehmens, die in der Sicherheits-, Kontinuitäts- und Risikopolitik ihren Niederschlag finden. Auf diesen bauen die Sicherheitsziele bzw. -anforderungen der Geschäfts-, Support- und Begleitprozesse auf.

Um die Sicherheitsanforderungen der Prozesse erfüllen zu können, müssen diese auf jene Ressourcen abgebildet werden, die für die ordnungsmäßige Funktionsfähigkeit des jeweiligen Prozesses erforderlich sind. Dieser Vorgang ist in der Sicherheitspyramide durch die Ebene der Transformation dargestellt. Hieraus leiten sich die Sicherheitsarchitektur, -richtlinien, -konzepte und -maßnahmen ab. Risiken und Schwachstellen werden transparent, Sicherheitslücken können geschlossen werden.

Die zweite Dimension der Sicherheitspyramide berücksichtigt die erforderlichen Themen Prozesse, Ressourcen und Organisation für das Sicherheitsmanagement (PROSim).

*2. Dimension:
PROSim*

Die dritte Dimension behandelt die einzelnen Phasen im jeweiligen Prozess-, Ressourcen-, Dienstleistungs- oder Produktlebenszyklus, wobei Ressourcen z. B. Systeme sein können. Abhängig vom zugrunde liegenden Phasenmodell und der jeweiligen Ressource reichen die Phasen von der Idee über die Machbarkeitsstudie, die Anforderungsanalyse, Konzeption, Entwicklung, den Test, die Abnahme, die Inbetriebnahme und den Betrieb bis hin zur Außerbetriebnahme und Entsorgung. In jede Phase und jeden Prozess werden Sicherheitselemente integriert, um eine prozess- und lebenszyklusimmanente Sicherheit zu erreichen.

*3. Dimension:
Lebenszyklus*

Der Regelkreis umrahmt die Sicherheitspyramide. Er steuert den Aufbau, die Prüfung und die gezielte Weiterentwicklung sowie das Berichtswesen. Hierdurch lassen sich die Handlungsfähigkeit und das Image eines Unternehmens langfristig verbessern.

*Sicherheits-
regelkreis*

Der IT-Sicherheitsmanagementprozess einschließlich des Kontinuitäts- und Risikomanagementprozesses ermöglicht – aufbauend auf der Sicherheitspyramide des Autors – den Aufbau und Betrieb sowie die kontinuierliche Überwachung, Steuerung, Prüfung und Verbesserung der IT-Sicherheit und der Kontinuität im Unternehmen sowie der Risiken.

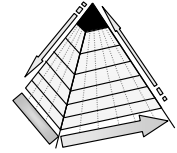
*Sicherheits-
management-
prozess*

Manch einen mag es wundern, wenn ich von der dreidimensionalen Sicherheitspyramide, dem dreidimensionalen Pyramidenmodell, u. ä. „spreche“, wo Pyramiden doch bekanntermaßen dreidimensional sind. Es handelt sich also um einen Pleonasmus, also eine sprachliche Redundanz. Warum verwende ich das Wort dreidimensional dann? Dies ist der explizite Hinweis darauf, dass die „Sicherheitspyramide“ des Autors tatsächlich drei Dimensionen besitzt.

Anmerkung

6 Sicherheits-, Kontinuitäts- und Risikopolitik

Die Kosten für Sicherheit sind ein immer wiederkehrendes leidiges Thema. Argumentationen laufen oftmals ins Leere, weil keine Transparenz über den Nutzen der Investitionen in die Sicherheit vorhanden ist und die aktuellen und zukünftigen Anforderungen und Risiken des Unternehmens nicht bekannt sind. Diese sind jedoch die Basis für Kosten-Nutzen-Betrachtungen.



Die Sicherheits- und Kontinuitätsanforderungen hängen ab von Gesetzen, vom Unternehmenszweck, der mittel- und langfristigen Ausrichtung, dem Umfeld und der strategischen Positionierung des Unternehmens. Möchte das Unternehmen im Vergleich zu Wettbewerbern Klassenbester („best of class“), d. h. risikoscheu, sein, oder ist es risikofreudig und begnügt sich beim Sicherheitsniveau mit einem der hinteren Plätze? Diese generelle Ausrichtung des Unternehmens bildet den Ausgangspunkt für die weiteren sicherheitsspezifischen Überlegungen. Das Top Management legt sie in der Sicherheits-, Kontinuitäts- und Risikopolitik und/oder in entsprechenden Leitsätzen bzw. Leitlinien fest.

Gesetzliche Anforderungen

Im Aktiengesetz §93, Stand: 19.4.2007, heißt es: „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. [...] Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet.“



Gesetzliche Anforderungen zur Sorgfaltspflicht und Haftung

Die folgenden Unterkapitel beschäftigen sich mit diesen Aspekten der Sicherheits-, Kontinuitäts- und Risikopolitik:

1. Zielsetzung
2. Umsetzung
3. Inhalte
4. Checkliste
5. Praxisbeispiele
6. Zusammenfassung

6.1 Zielsetzung

Wozu braucht ein Unternehmen ein Sicherheits-, Kontinuitäts- und Risikomanagement und welche Ziele verfolgt es damit? Die Notwendigkeit ergibt sich aus der Absicherung des Unternehmens, seiner Mitarbeiter und der Unternehmenswerte gegenüber den vielfältigen Bedrohungen, die von kriminellen Handlungen über infrastrukturelle, technische und personelle Ausfälle bis hin zu höherer Gewalt reichen. Hieraus ergeben sich als Ziele die Einhaltung von Gesetzen und vergleichbaren Vorgaben sowie die Erfüllung der unternehmensspezifischen Anforderungen.

Art und Umfang des Sicherheits-, Kontinuitäts- und Risikomanagements sowie die damit verbundenen Investitionen haben hierbei eine große Bandbreite. Um diese einzuschränken und das Unternehmen dementsprechend auszurichten, müssen die aktuellen und zukünftigen geschäftspolitischen Anforderungen des Unternehmens an das Sicherheits-, Kontinuitäts- und Risikomanagement festgelegt und kommuniziert werden.

Weiterhin ist es notwendig, das Management und alle Mitarbeiter für das Thema Sicherheit zu sensibilisieren und sie in das Sicherheits-, Kontinuitäts- und Risikomanagement einzubinden. Das Management und hierbei insbesondere die Geschäftsleitung soll darin eine Führungsrolle und Vorbildfunktion übernehmen und die benötigten Mittel und Ressourcen bereitstellen.

6.2 Umsetzung

*Unternehmens-
weite
Sicherheits-,
Kontinuitäts-
und Risiko-
politik*

Diese Ziele werden dadurch anvisiert, dass sich das Unternehmen eine unternehmensweite Sicherheits-, Kontinuitäts- und Risikopolitik gibt. In ihr stellt das Top Management – abgeleitet vom Unternehmenszweck und der Unternehmensstrategie – dar, welche Sicherheitskriterien für das Unternehmen kurz-, mittel- und langfristig welche Bedeutung haben und wie die Sicherheitspolitik umgesetzt werden soll. Ebenfalls dargelegt wird, wie sich das Unternehmen risikopolitisch aufstellt, d. h. ist es eher risikofreudig oder risikoscheu, setzt es eher auf Prävention oder auf Postvention, versucht es Trends und Ereignisse zu antizipieren oder auf sie zu reagieren?

Das Top Management bringt in der Sicherheits-, Kontinuitäts- und Risikopolitik zum Ausdruck, dass es sich selbst an die Spitze des Sicherheitsmanagements stellt und dass jeder Mitarbeiter seinen Beitrag zur Sicherheit leisten muss. Das Management und hierbei insbesondere die Geschäftsleitung übernehmen eine Führungsrolle und

Vorbildfunktion im Sicherheitsmanagement und stellen die benötigten Mittel und Ressourcen bereit.

Argumente für eine Sicherheits-, Kontinuitäts- und Risikopolitik

Eine fehlende Sicherheits-, Kontinuitäts- und Risikopolitik kann – wie mehrfach erlebt – dazu führen, dass jeder Verantwortliche sich selbst die fehlenden Vorgaben definiert. Diese sind im Unternehmen dann verstreut innerhalb einer Vielzahl von Dokumenten zu finden. Die individuellen Vorgaben sind üblicherweise inkonsistent zueinander und weichen von den Vorstellungen des Top Managements ab. Ohne Sicherheits-, Kontinuitäts- und Risikopolitik fehlt den Mitarbeitern darüber hinaus eine Orientierung, ein diesbezüglicher Verhaltenskodex und die erforderliche Sensibilisierung. Dies kann dazu führen, dass der Fokus auf der kurzfristigen Gewinnoptimierung liegt und die angemessene Absicherung für das mittel- und langfristige Überleben des Unternehmens in den Hintergrund tritt.

Ohne Vorgaben entwickeln die jeweils Verantwortlichen für ihr Aufgabengebiet individuell beispielsweise Gliederungsstrukturen und generelle Inhalte von Prozessbeschreibungen, Katastrophenvorsorgehandbüchern, Wiederanlaufplänen usw. Dies bedeutet Doppelarbeit und ist damit ineffizient. Außerdem sind die einzelnen Beschreibungen, Handbücher und Pläne unterschiedlich aufgebaut und haben einen voneinander abweichenden Detaillierungs- und Vollständigkeitsgrad. Dies führt zu Nacharbeiten, die zusätzliches Budget erfordern und die Motivation der Mitarbeiter senken können.

Nicht zuletzt fordern nationale und internationale Standards und Practices eine Sicherheits- und/oder Kontinuitätspolitik.



Argumente

Die Darstellungen in der Sicherheits-, Kontinuitäts- und Risikopolitik sind überblicksartig und geben einen Orientierungsrahmen vor, enthalten somit noch kaum detaillierte Angaben. Hierdurch erreicht die Geschäftsleitung, dass die Sicherheits-, Kontinuitäts- und Risikopolitik, die von ihr selbst unterschrieben wird, mittel- bis langfristig Bestand hat.

*Orientierungs-
rahmen*

Neben der Sicherheits-, Kontinuitäts- und Risikopolitik, die auf wenigen Seiten zusammengefasst sein sollte, empfiehlt sich ein „sicherheitspolitischer Leitsatz“. Er bringt die Sicherheitspolitik kurz, prägnant und eingängig auf den Punkt.

*Sicherheits-
politischer
Leitsatz*

6.3 Inhalte

Nachdem die Geschäftsleitung den Rahmen für die Sicherheits-, Kontinuitäts- und Risikopolitik festgelegt hat, stellt sich die Frage, welche

Themen

konkreten Themen sie dort direkt oder referenziert ansprechen sollte. Diese Themen sind im Folgenden überblicksartig angegeben:

- Aufgabe bzw. Mission sowie Vision und Strategie des Unternehmens
- Informationen über die Kundenanforderungen
- externe Sicherheits- und Kontinuitätsanforderungen durch Gesetze, Vorschriften, Ausführungsbestimmungen, Prüfungsrichtlinien, Normen und Standards
- allgemeine Sicherheits-, Kontinuitäts- und Risikoziele, d. h. die Bedeutung der zusammenhängenden Themen Sicherheit, Kontinuität und Risiko für das Unternehmen
- Angaben zur Bereitstellung der erforderlichen Mittel und Ressourcen durch das Top Management
- Bedeutung der verschiedenen Sicherheitskriterien für das Unternehmen
- Übergreifende Ziele und Vorgaben zur Sicherheit (was soll erreicht werden), welche die Basis für die Ableitung der Sicherheitsanforderungen innerhalb des Unternehmens bilden
- abzusichernde Mindestszenarien und zu betrachtender Planungshorizont für die Notfall- und Katastrophenvorsorgeplanung
- Sicherheitsklassen und zugeordnete Schadenshöhen
- Sicherheits-, Kontinuitäts- und Risikomanagementprozess
- Vorgehensweise
- übergreifende Prinzipien, z. B. Vier-Augen-Prinzip, Prinzip des generellen Verbots, der minimalen Rechte und Dienste, der Funktionstrennung, des „gesperrten Bildschirms“ und des „aufgeräumten“ Arbeitsplatzes
- Hinweise zu den Beteiligten, deren Aufgaben und Verantwortlichkeiten
- Hinweise zu Sensibilisierung, Schulung und Übung
- Hinweise zur Prüfung, Aktualisierung, Pflege und Weiterentwicklung
- Verpflichtung des Top Managements und der Mitarbeiter auf die Einhaltung und Fortentwicklung der Sicherheitsregeln.
- Nachweisfähigkeit
- Transparenz, Durchgängigkeit und Systematik
- Wirtschaftlichkeit

Bei der Gestaltung der Sicherheits-, Kontinuitäts- und Risikopolitik spielen die Branche, die Mission des Unternehmens und seine strategische Positionierung im Markt eine wesentliche Rolle. Bei Banken bestehen insbesondere im Zahlungsverkehr, aber auch beim Wertpapierhandel im Hinblick auf die Positionsführung der Bank höchste Anforderungen an die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten. Extrem hohe Anforderungen an Kontinuität und Verfügbarkeit, aber auch hohe Anforderungen an die Integrität und Vertraulichkeit der Daten stellen Kreditkartenprozessoren im Rahmend es Online-Transaction-Processing (OTP).

Branchen- und unternehmensspezifische Sicherheits-, Kontinuitäts- und Risikopolitik

Bei gesetzlichen Krankenversicherungen ist neben dem Bundesdatenschutzgesetz (BDSG) der Sozialdatenschutz (SGB X) ein wesentliches Element der Sicherheit. Auch die Verfügbarkeit spielt im Hinblick auf die zeitnah an die Sozialversicherungen zu transferierenden jährlichen Milliardenbeträge eine wichtige Rolle.

6.4 Checkliste

Checkliste mit Kontrollen (Controls) zur Sicherheits-, Kontinuitäts- und Risikopolitik	Zwingend/ Optional	Ja (✓) / Nein (-)
Verfügt das Unternehmen über eine <u>Sicherheits-, Kontinuitäts- und Risikopolitik</u> ?	Z	
Verfügt das Unternehmen über einen <u>sicherheitspolitischen Leitsatz</u> ?	O	
Erfolgt die <u>Freigabe der Sicherheits-, Kontinuitäts- und Risikopolitik</u> vom Top Management?	Z	
Leitet sich die Sicherheits-, Kontinuitäts- und Risikopolitik aus dem <u>Unternehmenszweck, der Vision und der Strategie des Unternehmens ab</u> ?	Z	
Sind Informationen über die <u>Kundenanforderungen</u> enthalten sowie gegebenenfalls über Anforderungen weiterer Bezugsgruppen, wie Mitarbeiter und Anteilseigner?	O	
Enthält die Sicherheits-, Kontinuitäts- und Risikopolitik eine Anlage mit Hinweisen zu Sicherheitsanforderungen durch <u>Gesetze, Vorschriften, Ausführungsbestimmungen, Prüfungsrichtlinien, Normen und Standards</u> ?	Z	
Stellt die Sicherheits-, Kontinuitäts- und Risikopolitik die <u>Bedeutung des Themas Sicherheit einschließlich Kontinuität</u> für das Unternehmen dar?	Z	
Geht die Sicherheits-, Kontinuitäts- und Risikopolitik des Unternehmens auf die <u>Bedeutung der verschiede-</u>	Z	

Checkliste mit Kontrollen (Controls) zur Sicherheits-, Kontinuitäts- und Risikopolitik	Zwingend/ Optional	Ja (✓) / Nein (-)
<u>nen Sicherheitskriterien</u> Konformität, Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit ein?		
Hat die Geschäftsleitung <u>die abzusichernden Mindestszenarien und den abzusichernden Mindestzeitraum</u> (Planungshorizont) definiert? – Sind diese als vertraulich gekennzeichnet?	Z	
Hat die Geschäftsleitung die <u>Sicherheitsklassen mit den damit verbundenen Schadenshöhen</u> verabschiedet? – Sind diese als vertraulich gekennzeichnet?	Z	
Macht die Sicherheits-, Kontinuitäts- und Risikopolitik <u>übergreifende Ziele und Vorgaben</u> zur Sicherheit, aus denen sich die Sicherheits- und Kontinuitätsanforderungen innerhalb des Unternehmens ableiten lassen?	Z	
Enthält die Sicherheits-, Kontinuitäts- und Risikopolitik Informationen zum <u>Sicherheits-, Kontinuitäts- und Risikomanagementprozess sowie zum Vorgehensmodell</u> für das Sicherheits-, Kontinuitäts- und Risikomanagement?	Z	
Nennt die Politik <u>übergreifende Prinzipien</u> , z. B. Vier-Augen-Prinzip, Prinzip des generellen Verbots, der minimalen Rechte und Dienste, der Funktionstrennung, des „gesperrten Bildschirms“ und des „aufgeräumten“ Arbeitsplatzes?	O	
Enthält die Sicherheits-, Kontinuitäts- und Risikopolitik Hinweise auf <u>Sensibilisierung, Schulung und Übung</u> ?	Z	
Gibt die Politik Hinweise zur <u>Prüfung, Aktualisierung, Pflege und Weiterentwicklung</u> des Sicherheits-, Kontinuitäts- und Risikomanagements?	Z	
Enthält die Sicherheits-, Kontinuitäts- und Risikopolitik überblicksartige Angaben zu den <u>Beteiligten, deren Aufgaben und Verantwortlichkeiten sowie zu deren Rang</u> ?	Z	
Erklärt sich das Top Management bereit, die erforderlichen <u>Mittel und Ressourcen</u> für das Sicherheits-, Kontinuitäts- und Risikomanagement bereitzustellen?	Z	
Ist eine <u>Verpflichtung des Top Managements und der Mitarbeiter</u> zur Sicherheit enthalten?	Z	
Ist die <u>Nachweisfähigkeit</u> gefordert?	Z	

Checkliste mit Kontrollen (Controls) zur Sicherheits-, Kontinuitäts- und Risikopolitik	Zwingend/ Optional	Ja (✓) / Nein (-)
Enthält die Sicherheits-, Kontinuitäts- und Risikopolitik die Forderung nach Transparenz, Durchgängigkeit und Systematik?	Z	
Hat die Geschäftsleitung das Thema <u>Wirtschaftlichkeit</u> angesprochen?	Z	

6.5 Praxisbeispiele

Wie kann ein sicherheitspolitischer Leitsatz oder die Sicherheits-, Kontinuitäts- und Risikopolitik in der Praxis aussehen? Die folgenden auszugsweisen Beispiele geben Ihnen Anregungen.

6.5.1 Sicherheits-, kontinuieräts- und risikopolitische Leitsätze Versicherung

Sicherheits-, kontinuieräts- und risikopolitische Leitsätze

Wir, die <Musterversicherung>, bieten unseren Kunden eine breite Palette von Versicherungsleistungen an. Unsere Versicherten erwarten eine vertrauliche Behandlung ihrer Daten, zeitnahe Auskunftsfähigkeit über ihre Versicherungen, gute Erreichbarkeit und schnelle Schadensregulierung. Unsere Außendienstorganisation erwartet eine tägliche Verfügbarkeit der ITK-Systeme.

Unsere Kunden, Anteilseigner und Mitarbeiter erwarten Zukunftssicherheit unseres Unternehmens und damit jederzeitige Handlungsfähigkeit und Wirtschaftlichkeit sowie Gesetzeskonformität. Transparenz über die Risikosituation ist eine weitere Forderung.

Unser unternehmensweites Sicherheits-, Kontinuitäts- und Risikomanagement verfolgt folgende Ziele:

1. Schutz von Personen
2. Schutz von Unternehmenswerten
3. Existenzsicherung des Unternehmens
 - Erhalt der Handlungs- und Überlebensfähigkeit des Unternehmens auch in Not- und Katastrophenfällen
 - Erhalt und Ausbau des Unternehmenserfolgs
 - Erhalt und Ausbau des Images
4. Einhaltung von Gesetzen und vergleichbaren Vorgaben, wie z. B. durch Aufsichtsbehörden und Wirtschaftsprüfer
5. Erfüllung von Verträgen
6. Nachweisfähigkeit
7. Transparenz, Durchgängigkeit und Systematik

8. Wirtschaftlichkeit, d. h. die ökonomisch angemessene Erfüllung der relevanten Anforderungen unserer Zielkunden, Anteilseigner und Mitarbeiter.

Unser Ziel ist es, Bedrohungen und Risiken vorausschauend zu erkennen und angemessen abzusichern. Bei vergleichbarer Kosten-Nutzen-Situation geben wir der Vermeidung durch Prävention den Vorrang vor Wiederherstellung.

Im Hinblick auf sicherheitsrelevante Ereignisse betrachten wir folgende Themen: Vorbeugung, Beobachtung, Erkennung, Meldung/Alarmierung, Erwidern, Beurteilung, Wiederherstellung, Verbesserung, Nachvollziehbarkeit, Nachweisbarkeit, Sensibilisierung und Übung.

Um die genannten Ziele zu erreichen, ermitteln wir die Sicherheitsanforderungen unserer Geschäftsprozesse entsprechend ihrer Bedeutung für das Unternehmen. Den Anforderungen gemäß klassifizieren wir sie und die von ihnen benötigten Ressourcen. Wir berücksichtigen hierbei Anforderungen von Gesetzen und Vorgaben der Aufsichtsbehörden.

Wir verschaffen uns einen Überblick über die potenziellen Bedrohungen und Risiken. Die Risiken fassen wir in einem Risikoinventar zusammen.

In Abhängigkeit von den Sicherheitsanforderungen entwickeln wir für die Geschäftsprozesse und ihre Ressourcen Sicherheitsrichtlinien und -konzepte. Diese setzen wir in Form von Maßnahmen um. Wir prüfen, verfolgen und steuern das Sicherheits-, Kontinuitäts- und Risikomanagement und entwickeln es kontinuierlich anforderungsgerecht und wirtschaftlich weiter.

Wir wollen ein – unter Kosten-Nutzen-Aspekten – optimiertes Sicherheitsniveau erreichen. Hierzu gehört, dass die Einhaltung vorgegebener Sicherheitsregeln weitestgehend automatisch bewirkt und überprüft wird.

Weiterhin wenden wir in allen Bereichen das Prinzip des generellen Verbots an, das besagt, dass alles verboten ist, was nicht explizit erlaubt ist. Durch das Prinzip der minimalen Rechte, gewähren wir Zufahrt, Zutritt, Zugang und Zugriff nur in dem Umfang, wie dies zur Erfüllung der Aufgaben erforderlich ist. Wir verfolgen das Prinzip des „aufgeräumten Arbeitsplatzes“ und des „gesperrten Bildschirms“, sodass für Unberechtigte keine Unterlagen offen zugänglich sind. Für die Aufgabenerfüllung wird stets nur die vom Unternehmen bereitgestellte Infrastruktur (z. B. Hard- und Software) genutzt.

Alle Mitarbeiter verpflichten sich, auf sicherheitsrelevante Ereignisse zu achten und sie zu melden, sich jederzeit sicherheits- und risikobewusst zu verhalten sowie die hier genannten Anforderungen und die Sicherheitsregelungen der <Musterversicherung> einzuhalten.

<Musterort>, <Musterdatum>

<Mustergeschäftsführung>

6.5.2 Sicherheits-, Kontinuitäts- und Risikopolitik

Das folgende prinzipielle und auszugsweise Beispiel einer Sicherheits-, Kontinuitäts- und Risikopolitik für ein Unternehmen ist im Sinne einer knappen und fortlaufenden Beschreibung aufgebaut. Alternativ lässt sich diese Politik durch eine Gliederung und einzeln identifizierbare Unterpunkte stärker formalisieren und detaillieren. Wichtig bei der Formulierung der Sicherheits-, Kontinuitäts- und Risikopolitik sowie ihrem Umfang und Inhalt sind die Zielgruppen, deren Interessen und Sprachgebrauch. Wenngleich in diesem Buch das Thema Sicherheit über das Sicherheitskriterium Verfügbarkeit den Themenkomplex Kontinuität enthält, ist er in dieser Politik im Hinblick auf deren Leser an verschiedenen Stellen zusätzlich explizit ausgewiesen.

Sicherheits-, Kontinuitäts- und Risikopolitik

Die vorliegende Sicherheits-, Kontinuitäts- und Risikopolitik legt fest,

1. welchen Unternehmenszweck wir verfolgen,
2. wer unsere Zielkunden und Bezugsgruppen sind,
3. welche Anforderungen und Ziele sich daraus für das Sicherheits-, Kontinuitäts- und Risikomanagement ergeben und
4. wie wir das Sicherheits-, Kontinuitäts- und Risikomanagement aufbauen, einführen, pflegen und weiterentwickeln, um diese Anforderungen kontinuierlich zu erfüllen.

Unternehmenszweck

Wir, die <Musterbank>, bieten unseren Kunden eine breite Palette von Finanzdienstleistungen an. Für unsere Zielkunden sind wir die „erste Adresse“ und wollen diese Position für die Zukunft weiter ausbauen.

Zielkunden

Unsere Zielkunden sind vermögende Privatkunden und anspruchsvolle Großunternehmen. Sie erwarten von uns absolute Diskretion (*Vertraulichkeit*), korrekte Auftragsabwicklung (*Integrität und Verbindlichkeit*) und die Möglichkeit, ihre Finanztransaktionen über unterschiedliche Kommunikationskanäle (Multi-Channel-Processing) sicher (*Vertraulichkeit, Integrität und Verbindlichkeit*) und jederzeit (*Verfügbarkeit und Kontinuität*) durchführen zu können.

Bezugsgruppen

Unsere Bezugsgruppen, wie z. B. Kunden, Anteilseigner und Mitarbeiter, fordern Zukunftssicherheit der <Musterbank>, d. h. die Einhaltung von Gesetzen und Vorgaben sowie die jederzeitige angemessene Handlungsfähigkeit und Existenzsicherung. Gleichzeitig erwarten sie jederzeitige Transparenz über unsere Risikosituation.



Sicherheitsziele/Sicherheitsanforderungen

Aus diesen Anforderungen leiten wir folgende Ziele unseres Sicherheits-, Kontinuitäts- und Risikomanagements ab:

1. Einhaltung relevanter Gesetze und vergleichbarer Vorgaben, wie z. B. durch Aufsichtsbehörden und Wirtschaftsprüfer. An den verschiedenen Standorten des Unternehmens berücksichtigen wir die jeweiligen bundesland- und landesspezifischen Gesetze und Vorschriften. Relevante Gesetze und vergleichbare Vorgaben sind in der Anlage 1 auszugsweise und überblicksartig zusammengestellt.
2. Schutz von Personen
3. Schutz von Unternehmenswerten
4. Existenzsicherung des Unternehmens
 - Erhalt der Handlungs- und Überlebensfähigkeit des Unternehmens auch in Not- und Katastrophenfällen.
 - Erhalt und Ausbau des Unternehmenserfolgs
 - Erhalt und Ausbau des Images
 - Handeln zum Wohle des Unternehmens auf Basis angemessener Informationen und ohne Eigeninteressen, ohne Interessenkonflikte und ohne Fremdeinflüsse sowie in gutem Glauben
5. Erfüllung von Verträgen
6. Früherkennung und kontinuierliches Monitoring
7. Nachweisfähigkeit
8. Transparenz, Durchgängigkeit und Systematik
9. Sicherheitsfördernde Unternehmenskultur
10. Wirtschaftlichkeit, d. h. die ökonomisch angemessene Erfüllung unserer Anforderungen sowie der relevanten Anforderungen unserer Zielkunden, Anteilseigner und Mitarbeiter

Aufgrund unseres Unternehmenszwecks und Selbstverständnisses positionieren wir uns im Sicherheits- und Kontinuitätsniveau als Klassenbester und streben ein entsprechend niedriges Risikoniveau an. Dennoch nehmen wir bei entsprechenden Chancen auch angemessene Risiken auf uns. Wir stellen jederzeit sicher, dass wir keine existenzgefährdenden Risiken eingehen. Als Risikostrategie vermeiden, verringern, verlagern oder vereinnahmen wir Risiken, soweit dies sinnvoll und wirtschaftlich angemessen ist. Bei vergleichbarer Kostensituation ziehen wir Prävention der Postvention vor.

Unsere Risiken sind im Risikoportfolio zusammen mit Risikogrenzwerten dargestellt, die wir in der Risikolandkarte (Risk Map) visualisieren. Wir haben einen Risikomanagementprozess etabliert und steuern unser Risikoniveau.

Den Anforderungen unserer Zielkunden entsprechend haben Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit, aber auch Nachvollziehbarkeit und Nachweisbarkeit einen sehr hohen Stellenwert.

Wenn erforderlich oder ökonomisch sinnvoll berücksichtigen wir nationale und internationale Normen, Standards und Practices (s. Anlage 2).

Verantwortung der Geschäftsleitung

Aus den Unternehmensanforderungen, den Gesetzen und Vorschriften sowie unseren unternehmensspezifischen Zielen leitet die Geschäftsleitung die Sicherheitskriterien und deren Wichtigkeit für das Unternehmen ab.

Sie definiert die Sicherheits-, Kontinuitäts- und Risikopolitik, die Risikogrenzwerte, die abzusichernden Mindest- und Grenzszenarien und den Zeithorizont der Notfall- und Katastrophenvorsorgeplanung. Die Geschäftsleitung verabschiedet den Sicherheits-, Kontinuitäts- und Risikomanagementprozess, die Vorgehensweise sowie die Sicherheits- bzw. Risikoklassen einschließlich der damit verbundenen Schadenshöhen. Darüber hinaus stellt sie die erforderlichen Mittel und Ressourcen für das Sicherheits-, Kontinuitäts- und Risikomanagement bereit und fördert eine jederzeit faire, partnerschaftliche und leistungsorientierte Unternehmenskultur.

Vorgehensmodell

Als strukturierten und strategischen Ansatz für das Sicherheits-, Kontinuitäts- und Risikomanagement sowie das Konformitätsmanagement haben wir die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller gewählt. Dies ermöglicht es uns, das Sicherheits-, Kontinuitäts- und Risikomanagement ganzheitlich und integrativ top-down aufzubauen, zu steuern und weiterzuentwickeln, die Themenfelder Prozesse, Ressourcen und Organisation zu berücksichtigen sowie produkt-, leistungs-, prozess-, ressourcen- und lebenszyklusimmanente Sicherheit zu erreichen. Durch die integrative Nutzung der gleich aufgebauten dreidimensionalen Kontinuitäts- und Risikomanagementpyramiden nach Dr.-Ing. Müller synchronisieren wir unser Sicherheits-, Kontinuitäts- und Risikomanagement.

Sicherheits-, Kontinuitäts- und Risikomanagementprozess

Unser Sicherheits-, Kontinuitäts- und Risikomanagementprozess orientiert sich am Plan-Do-Check-Act-Zyklus. Die Planungsphase dient dem erstmaligen und später dem weiterentwickelnden Aufbau des Sicherheits-, Kontinuitäts- und Risikomanagements (SKRM) gemäß der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller einschließlich entsprechender Kontrollen. In der Durchführungsphase schulen, kommunizieren und testen wir das SKRM-System. Diese Phase enthält weiterhin das Monitoring, Controlling und Reporting ausgerichtet am Sicherheitsregelkreis der Sicherheitspyramide sowie Pflege, regelmäßige Sensibilisierung und Übung. In der Prüfungsphase (Check) führt die Geschäftsleitung jährlich ein Review durch. Außerdem finden unterjährig geplante und bedarfsorientierte Prüfungen, Analysen und Bewertungen des SKRM statt. In der Aktionsphase identifizieren wir Verbesserungspotenziale sowie präventive und korrigierende Aktivitäten. Diese priorisieren wir und genehmigen sie unter Kosten-Nutzen-Aspekten.

Sicherheitsanforderungen und Risikoziele

Das Sicherheits-, Kontinuitäts- und Risikoniveau soll unsere und die Anforderungen unserer Zielkunden in gesetzeskonformer und ökonomischer Weise nachvollziehbar erfüllen. Um dies zu erreichen, definieren wir je Sicherheitskriterium Sicherheitsklassen und deren Charakteristika sowie je Risikokategorie Risikoklassen und deren Charakteristika. Sicherheits-, Kontinuitäts- und Risikoklassen verknüpfen wir miteinander bzw. integrieren sie. Kontinuitätsklassen entsprechen den Verfügbarkeitsklassen.

Basis unseres Unternehmens sind die Geschäftsprozesse. Diese sind in der Geschäftsprozessarchitektur dokumentiert. Für jeden Geschäftsprozess erheben wir die Sicherheitsanforderungen mittels einer Geschäftseinflussanalyse. Hierbei beachten wir die Vorgaben aus der Sicherheits-, Kontinuitäts- und Risikopolitik.

Wir definieren Sicherheitsklassen und klassifizieren die Geschäftsprozesse gemäß ihren Sicherheits- und Kontinuitätsanforderungen. Da die Geschäftsprozesse Ressourcen, z. B. Räumlichkeiten und Computersysteme, nutzen, leiten wir deren Sicherheitsklasse aus den Anforderungen des jeweiligen Geschäftsprozesses ab. Die Aufrechterhaltung der Geschäftsprozesse erfordert den Schutz dieser Ressourcen. Wir nennen diese Ressourcen daher Schutzobjekte.

Da sich gleichartige Schutzobjekte auf ähnliche Weise absichern lassen, bilden wir Schutzobjektklassen. Schutzobjektklassen sind Personen, Gebäude, Räumlichkeiten, haustechnische Infrastruktur, Informations- und Kommunikationssysteme, Materialien, finanzielle Mittel, interne und externe Services sowie Know-how.

In diesem Zusammenhang legen wir den Planungshorizont für die Notfall- und Katastrophenvorsorge sowie für jeden Geschäftsprozess den zeitlich gestaffelten Mindestgeschäftsbetrieb fest, der in Notsituationen zur Aufrechterhaltung unserer Handlungsfähigkeit erforderlich ist.

Sicherheits-, Kontinuitäts- und Risikotransformation

Durch eine Transformation bilden wir die Sicherheits- und Kontinuitätsanforderungen der Geschäftsprozesse auf Sicherheits- und Kontinuitätselemente für die Prozesse selbst und für die Schutzobjekte ab. Hierbei unterscheiden wir in Maßnahmen, die vorbeugend, beobachtend, erkennend, meldend, abwehrend, schadensbeurteilend und wiederherstellend sind. In entsprechender Weise transformieren wir die Risikoziele.

Sicherheits- und Kontinuitätsarchitektur, -richtlinien, -konzepte und -maßnahmen

In der Sicherheits- und Kontinuitätsarchitektur stellen wir das Spektrum an Sicherheits- und Kontinuitätselementen strukturiert dar und definieren die relevanten Prozesse, insbesondere auch für das Sicherheits-, Kontinuitäts- und Risikomanagement. Wir visualisieren die bestehende Sicherheits-, Kontinuitäts- und Risikoarchitektur, definieren Richtlinien und setzen diese in Form von spezifischen Konzepten und Maßnahmen um. Die Si-

cherheits- und Kontinuitätsrichtlinien, -konzepte und -maßnahmen entsprechen den jeweiligen risikomindernden Ebenen der Risikomanagementpyramide nach Dr.-Ing. Müller.

Lebenszyklusimmanentes Sicherheits-, Kontinuitäts- und Risikomanagement

Wir integrieren Sicherheits-, Kontinuitäts- und Risikoaspekte in den Lebenszyklus von Prozessen, Dienstleistungen, Produkten und Ressourcen, wie z. B. Anlagen und Systemen. So lassen sich Sicherheits-, Kontinuitäts- und Risikoaspekte von Anfang an mit betrachten und in den folgenden Lebenszyklusphasen weiter verfeinern. Elemente des Risikomanagements integrieren wir so in den Lebenszyklus, dass eine frühzeitige Risikoerkennung sowie eine gezielte Steuerung möglich sind.

Prozess- und ressourcenimmanentes Sicherheits-, Kontinuitäts- und Risikomanagement

Wir definieren und gestalten unsere Prozesse so, dass sie durch ihr Vorhandensein und in ihrem Ablauf sowie in den genutzten Ressourcen die erforderlichen Elemente für das Sicherheits-, Kontinuitäts- und Risikomanagement enthalten. So entsteht eine prozess- und ressourcenimmanente Sicherheit. Dementsprechend verfügen wir u. a. über die Begleitprozesse Konformitäts- und Datenschutzmanagement sowie Leistungsmanagement. Diese stellen sicher, dass das Sicherheits-, Kontinuitäts- und Risikomanagement sowie das Konformitäts- und Datenschutzmanagement auch bei der Auslagerung von Leistungen von Anfang an berücksichtigt werden.

Sicherheitsschalenmodell

Zum Schutz der Personen und der Unternehmenswerte nutzen wir das Sicherheitsschalenmodell nach Dr.-Ing. Müller. Ausgehend vom Objektschutz als äußerster Schale, sichern wir die Zufahrt ab sowie über den Zutrittsschutz den Zutritt zu unserem Gebäude und den Räumlichkeiten. Den Zugang zu Informationssystemen und Netzen sichert der Zugangsschutz. Der Zugriffsschutz reglementiert den Zugriff auf Daten. Durch den Leseschutz verbergen wir Informationen vor Unbefugten. Vor der anderweitigen Verwendung oder Entsorgung von Datenträgern löschen wir diese oder vernichten sie. Abzusendende Objekte, Unterlagen und Daten prüfen wir auf die Zulässigkeit des Versands und schützen sie durch die angemessene Absicherung des Transports bzw. der Datenübertragung. Den Abgang und die Abfahrt von Daten und Objekten prüfen wir bei Bedarf auf Zulässigkeit.

Sicherheitsprinzipien

Wir wenden das Prinzip des generellen Verbots an. Es besagt, dass alles verboten ist, was nicht explizit erlaubt ist. Wir nutzen das Prinzip der minimalen Rechte, d. h. wir gewähren Zufahrt, Zutritt, Zugang und Zugriff nur in dem Umfang, wie dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist. Die Rechte ordnen wir Rollen zu. Mitarbeiter können eine oder mehrere Rollen wahrnehmen. Darüber hinaus setzen wir das Prinzip der minimalen Dienste, des „aufgeräumten Arbeitsplatzes“ und des „gesperr-

ten Bildschirms“ um, sodass für Unberechtigte Unterlagen und Informationen nicht offen zugänglich sind.

Organisation

Unsere interne Organisation mit Beteiligten, Aufgaben und Verantwortlichkeiten berücksichtigt die sicherheits-, kontinuieräts- und risikospezifischen Aktivitäten. Oberste Verantwortung für das Sicherheits-, Kontinuitäts- und Risikomanagement trägt die Geschäftsleitung. Sie ernennt kompetente und angemessen ranghohe Führungskräfte als operativ Verantwortliche.

Kommunikation, Sensibilisierung, Sicherheits- und Risikokommunikation, Schulung und Übung

Wir kommunizieren unsere Sicherheits-, Kontinuitäts- und Risikopolitik sowie die Risikostrategie im Unternehmen und erzeugen das erforderliche Sicherheits-, Kontinuitäts- und Risikobewusstsein. Mittels Sensibilisierung, Sicherheits- und Risikokommunikation, Schulung und Übung schaffen wir Bewusstsein und Routine im Hinblick auf die Unternehmenssicherheit und erhalten diese.

Reviews, Assessments und Tests

Durch Reviews, Assessments und Tests verifizieren wir die entwickelten Konzepte und getroffenen Maßnahmen.

Monitoring, Controlling, Berichtswesen, Prüfung

Als Basis des Monitorings, Controllings und Reportings definieren wir Kontrollelemente und Kennzahlen. Durch Überwachung, Analyse und Auswertung sowie Prüfungen steuern wir unser Sicherheits-, Kontinuitäts- und Risikomanagement und entwickeln es anforderungsgerecht weiter.

Aktualisierung, Pflege und Weiterentwicklung

Aktualisierung, Pflege und Weiterentwicklung sind elementarer Bestandteil unseres Sicherheits-, Kontinuitäts- und Risikomanagements.

Sanktionen

Wir behalten uns vor, Verletzungen dieser Politik sowie sicherheits-, kontinuieräts- und risikorelevanter Regelungen zu ahnden und die Verantwortlichen haftbar zu machen, wenn uns dadurch nachweisbar finanzielle oder andere Schäden entstanden sind. Konsequenzen können straf-, zivil- oder arbeitsrechtlicher Natur sein.

Verpflichtung aller

Das Top Management und alle Mitarbeiter verpflichten sich, die sicherheits-, kontinuieräts- und risikorelevanten Regelungen zu beachten, auf sicherheitsrelevante Ereignisse zu achten und sie zu melden, sich jederzeit sicherheits- und risikobewusst zu verhalten und potenziellen Bedrohungen angemessen und vorausschauend entgegenzuwirken.

<Musterort>, <Musterdatum>

<Musterverstand>

Anlage 1

In Deutschland berücksichtigen wir insbesondere folgende gesetzliche Regelungen, Vorgaben durch die Aufsichtsbehörden und Ausführungsrichtlinien:

- Gesetze im Bereich der Arbeitssicherheit, z. B. Arbeitsschutzgesetz (ArbSchG), Arbeitssicherheitsgesetz (ASiG)
- Allgemeines Gleichbehandlungsgesetz (AGG)
- Bürgerliches Gesetzbuch (BGB)
- Handelsgesetzbuch (HGB), Aktiengesetz (AktG)
- Kreditwesengesetz (KWG), Geldwäschegesetz (GwG), Wertpapierhandelsgesetz (WpHG)
- Bundesdatenschutzgesetz (BDSG), Teledienstschutzgesetz (TDDSG)
- Teledienstgesetz (TDG), Telemediengesetz (TMG)
- Urheberrechtsgesetz (UrhG)
- Markengesetz (MarkenG)
- Patentgesetz (PatG)
- Abgabenordnung (AO), Bankgeheimnis sowie Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Grundsätze ordnungsmäßiger Buchführung (GoB), Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV)
- Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW), z. B. Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie (FAIT 1), Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce (FAIT 2), Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)
- Abschlussprüfung bei Einsatz von Informationstechnologie (PS 330)
- Vorgaben der Aufsichtsbehörde (BaFin), z. B. die Mindestanforderungen an das Risikomanagement (MaRisk)
- Auslagerung von Bereichen auf ein anderes Unternehmen gemäß §25a, Abs. 2, KWG und Rundschreiben 11/2001, I3 – 272 A – 2/98 der BaFin/BaKred sowie Verlautbarung der BaFin/BaKred zur „Grenzüberschreitenden Datenfernverarbeitung im Bankbuchführungswesen“.

Anlage 2

Im Bereich der Informationsverarbeitung orientieren wir uns, u. a. zur Umsetzung der MaRisk-Anforderungen, an folgenden Normen, Standards, Methoden und Practices:

- den Control Objectives for Information and related Technology (COBIT®)
- der Information Security Governance des IT Governance Institute®

- der ISO/IEC 27001:2005
- der ISO/IEC 17799:2005 bzw. ISO/IEC 27002:2005
- der ISO/IEC 13335-1:2004
- dem IT-Grundschutzhandbuch des BSI
- der ISO/IEC 20000-1:2005 und 20000-2:2005
- dem BS 25999-1:2006
- dem BS 25999-2
- der IT Infrastructure Library (ITIL®)

6.6 Zusammenfassung

*Sicherheits-,
Kontinuitäts-
und Risiko-
politik:*

*Von Unterneh-
menszweck,
Vision und
Strategie zu
ganzheitlicher
prozess-,
ressourcen- und
lebenszyklus-
immanenter
Sicherheit*

Um das Sicherheits-, Kontinuitäts- und Risikomanagement zielgerichtet aufbauen, steuern und weiterentwickeln zu können, ist eine Sicherheits-, Kontinuitäts- und Risikopolitik für das Gesamtunternehmen erforderlich. Sie leitet sich aus dem Unternehmenszweck, den relevanten Anforderungen der Bezugsgruppen sowie der Vision und Strategie des Unternehmens ab. Sie wird vom Top Management verabschiedet, das sich zur Bereitstellung der Mittel und Ressourcen verpflichtet.

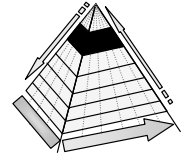
Die Sicherheits-, Kontinuitäts- und Risikopolitik stellt die Bedeutung der Sicherheit und spezieller Sicherheitskriterien für das Unternehmen sowie die Aufgaben des Unternehmens dar. Sie nimmt Bezug auf relevante Gesetze, Ausführungsrichtlinien, Normen, Standards und Good/Best Practices. Ferner erläutert sie generelle Sicherheitsziele, -strategien, -elemente und -prinzipien.

Zur Erreichung einer prozess-, ressourcen-, dienstleistungs- und produktimmanenten Sicherheit erfolgt die Orientierung an deren Lebenszyklus sowie die Berücksichtigung von prozessualen, ressourcenspezifischen und organisatorischen Aspekten. Ebenso werden die Beteiligten und ihre Aufgaben angesprochen.

Über die Sensibilisierung, Schulung und Übung hinaus thematisiert die Sicherheits-, Kontinuitäts- und Risikopolitik die Prüfung, den Test, die Aktualisierung, Pflege und Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements. Die Verpflichtung des Top Managements und aller Mitarbeiter auf die Sicherheit ist ebenfalls Bestandteil der Sicherheits-, Kontinuitäts- und Risikopolitik.

7 Sicherheitsziele / Sicherheitsanforderungen

Die Sicherheits-, Kontinuitäts- und Risikopolitik des vorangegangenen Kapitels legte die generellen Anforderungen und die Ausrichtung des Unternehmens im Hinblick auf Sicherheit fest. Ausgangspunkt waren hierbei der Unternehmenszweck, die Unternehmensziele sowie die erzeugten Produkte und/oder erbrachten Leistungen. Nun gilt es, die Sicherheits- und Kontinuitätsanforderungen zu konkretisieren, um sie später in Form von Richtlinien, Konzepten und Maßnahmen umsetzen zu können.



Ausgangsbasis sind die Kerngeschäfts-, Unterstützungs- und Begleitprozesse des Unternehmens, für die es einen Überblick, z. B. in Form einer Prozessarchitektur geben sollte. In dieser sind die Prozesse und ihre Bedeutung für das Unternehmen sowie ihr Zusammenwirken dargestellt. Für jeden Prozess sind Eckdaten (Prozesscharakteristika bzw. Prozessstammdaten) sowie die von ihm genutzten Ressourcen, wie z. B. Informations- und Kommunikationssysteme und Hilfsmittel, angegeben. Sollte das Unternehmen nicht prozessual organisiert sein, so kann alternativ von den Organisationseinheiten, den dort bearbeiteten Aufgaben und dem Zusammenspiel der verschiedenen Organisationseinheiten ausgegangen werden.

Die Zusammenstellung der Sicherheitsziele bzw. Sicherheitsanforderungen erfolgt anhand der Schutzbedarfsanalyse (Geschäftseinflussanalyse, Business Impact Analysis). Im ersten Schritt erheben die Prozessverantwortlichen den Schutzbedarf des jeweiligen Geschäftsprozesses insgesamt. Anschließend ermitteln sie den Schutzbedarf der einzelnen Prozessschritte, gefolgt von der Erhebung des Schutzbedarfs der genutzten Ressourcen (Schutzobjekte) im Rahmen einer Betriebseinflussanalyse (Operational Impact Analysis). Die folgenden Unterkapitel beschreiben die Erhebung der Sicherheitsziele bzw. -anforderungen:

1. Schutzbedarfsklassen
2. Schutzbedarfsanalyse (Prozessarchitektur, externe Sicherheitsanforderungen, Geschäfts- und Betriebseinflussanalyse)
3. Tabelle Schadensszenarien
4. Praxisbeispiel
5. Zusammenfassung

7.1 Schutzbedarfsklassen

*Schutzbedarfs-
vielfalt*

Um sich die Arbeit zu erleichtern, die Effizienz zu steigern und Vergleichbarkeit herzustellen, sollten Sie Schutzbedarfsklassen festlegen, bevor Sie mit der Schutzbedarfsanalyse beginnen. Der Schutzbedarf der verschiedenen Geschäfts- und Supportprozesse sowie der Schutzobjekte, wie z. B. der ITK-Systeme, ist üblicherweise unterschiedlich. Dementsprechend wären individuelle Sicherheitskonzepte und -maßnahmen erforderlich. Für jeden Geschäfts- und Supportprozess sowie für jedes ITK-System müssten individuelle Sicherheitskonzepte entwickelt, implementiert, gepflegt und geprüft werden. Durch die Vielzahl von Konzepten und Maßnahmen entstünde eine kaum mehr überschaubare Vielfalt: die Komplexität würde steigen, die Effizienz sinken.

*Schutzbedarfs-
klassen*

Um diesen Effekten entgegenzusteuern, werden für jedes Sicherheitskriterium Schutzbedarfsklassen geschaffen. Ihre Anzahl und Ausprägung orientiert sich an den unternehmensspezifischen Gegebenheiten, den Sicherheitsanforderungen und an Kosten-Nutzen-Aspekten.

In jeder Schutzbedarfsklasse ist festgelegt, welche Sicherheitsanforderungen sie erfüllt bzw. welche Auswirkungen von Sicherheitsverletzungen sie abdeckt.

Nun gilt es, Prozesse, Ressourcen, Produkte oder Dienstleistungen einer Schutzbedarfsklasse zuzuordnen. Hierzu konzentrieren wir uns auf die resultierenden Sicherheitsverletzungen, die durch eine der vielfältigen potenziellen Bedrohungen ausgelöst werden, z. B. einen Ausfall oder eine Blockade. Wir ermitteln deren Auswirkungen und leiten daraus die resultierenden Sicherheitsanforderungen ab.

7.2 Schutzbedarfsanalyse

Wie können Sie den Schutzbedarf erheben? Zuerst verschaffen Sie sich einen Überblick, welchen Zweck Ihr Unternehmen hat, welche Ziele es verfolgt, welche Produkte und/oder Leistungen es anbietet und wie es sich hinsichtlich Sicherheit, Kontinuität und Risikobereitschaft positioniert. Die Informationen hierzu finden Sie in der Unternehmensmission (mission statement) sowie in der zuvor behandelten Sicherheits-, Kontinuitäts- und Risikopolitik.

Im nächsten Schritt veranschaulichen Sie sich anhand der Prozessarchitektur, wie Ihr Unternehmen funktioniert. Für jeden Geschäftsprozess ermitteln Sie seine Bedeutung, d. h. seine Geschäftskritikalität (mission criticality). Die Bedeutung und damit der

Schutzbedarf ergibt sich, indem Sie die Folgen prinzipieller Sicherheitsverletzungen erheben, wie z. B. einer Störung, einer Unterbrechung, eines Ausfalls, aber auch einer Fehlbedienung, Verfälschung oder unberechtigten Einsichtnahme. Entsprechend den hierfür erforderlichen Schritten untergliedert sich dieses Kapitel in

1. Prozessarchitektur und Prozesscharakteristika,
2. Externe Sicherheitsanforderungen (z. B. Gesetze und Verordnungen),
3. Geschäftseinflussanalyse (Business Impact Analysis) und
4. Betriebseinflussanalyse (Operational Impact Analysis).

Praxistipp

Die Ergebnisse der Schutzbedarfsanalyse werden so festgehalten, dass berechnete Personen jederzeit auf sie zugreifen können. Es bietet sich an, diese Ergebnisse in einer Prozessinformations-Datenbank oder – wenn nicht vorgesehen – in einer Schutzbedarfsdatenbank abzulegen, auf die berechnete Personen über ein Portal im Intranet zugreifen können. Dieses sollte Informationen über Prozesse, ihre Prozessschritte und die genutzten Schutzobjekte enthalten. Hier empfiehlt es sich, auch die Prozess- und Schutzobjektverantwortlichen einzutragen.

Je Sicherheitskriterium sollte neben der Sicherheitsklasse des Prozesses auch die der Prozessschritte und der Schutzobjekte aufgenommen werden. Bei Ausfall eines Schutzobjekts, wie z. B. eines Servers, kann auf diesem Wege festgestellt werden, welche Informationssysteme und welche Geschäftsprozesse davon betroffen sind, und welche Sicherheitsanforderungen erfüllt werden müssen. Hierzu muss die Verfügbarkeit der Prozessinformationsdatenbank ihrerseits sicher gestellt sein.



Prozessinformationsdatenbank

7.2.1 Prozessarchitektur und Prozesscharakteristika

Voraussetzung für die Erhebung der Sicherheitsziele bzw. Sicherheitsanforderungen der Geschäftsprozesse ist ein Überblick über die vorhandenen Kerngeschäfts-, Unterstützungs- und Begleitprozesse, z. B. in Form einer Prozessarchitektur oder Prozesslandschaft. In dieser sind die Prozesse und ihr Zusammenspiel sowie die genutzten Ressourcen überblicksartig dargestellt.

Die Ermittlung der Prozesscharakteristika erfolgt für jeden Prozess in gleicher und standardisierter Form. Hierbei werden folgende Informationen erhoben:

Prozessarchitektur

Prozesscharakteristika

*Stammdaten,
Gesetze,
Schnittstellen,
Ressourcen,
Betriebs-
anforderungen*

- Stammdaten, z. B. Kerngeschäfts-, Unterstützungs- oder Begleitprozess, Umsatz/Budget, Deckungsbeitrag, strategische Bedeutung, Alleinstellungs- oder Abgrenzungsmerkmale zum Wettbewerb, Prozesseigentümer und dessen Stellvertreter
- externe Rahmenbedingungen, z. B. Gesetze, Vorschriften, Ausführungsbestimmungen, Standards, Normen
- Prozessablauf (Detaillierungsgrad gemäß Prinzip des „sachverständigen Dritten“)
- Verbindungsstellen (Schnittstellen) zu vorgelagerten, unterstützenden und nachgelagerten internen/externen Prozessen
- Art der genutzten bzw. bearbeiteten Daten, z. B. personenbezogene Daten, Sozialdaten oder Unternehmensdaten
- genutzte Ressourcen (Schutzobjekte) und deren Ausprägung, wie z. B. Anzahl und Qualifikationsprofil der Mitarbeiter, Größe und Lage der Gebäude sowie deren Infrastruktur, Größe und Anzahl der Räumlichkeiten und deren Infrastruktur, Ausstattung und Lage der Arbeitsplätze, genutzte Hilfs- und Arbeitsmittel, Anzahl und Leistungsfähigkeit eingesetzter Maschinen und Anlagen, Materialien, finanzielle Mittel, Art sowie Anzahl und Leistungsfähigkeit von Informations- und Kommunikationssystemen, interne und externe Services, Lieferanten, Versorgungsunternehmen und Know-how
- Nutzungsinformationen, z. B. Nutzungszeitraum täglich von ... bis ..., Anzahl Transaktionen, Durchsatz.

Jeder Prozess wird im Hinblick auf seine Bedeutung für das Unternehmen klassifiziert.

7.2.2 Externe Sicherheitsanforderungen

Leges et pacta sunt servanda.
(Gesetze und Verträge sind einzuhalten.)

*Implizite und
explizite
Sicherheits-
anforderungen*

Welche Sicherheitsanforderungen werden von externer Seite gestellt? Zuerst sind hier Gesetze, Verordnungen, Vorschriften und Ausführungsbestimmungen sowie aufsichtsbehördliche Anforderungen zu nennen. Hinzu kommen Normen und Standards, aber auch Anforderungen von Bezugsgruppen, wie z. B. Kunden und Anteilseignern. Diese können impliziter oder expliziter Natur sein. In impliziten Anforderungen spiegelt sich die unausgesprochene Erwartungshaltung des Kunden wider. Auch sie können bei Bedarf und entsprechendem Know-how der Auftragnehmer zumindest teilweise erfragt

und in explizite umgewandelt werden. Die implizite Erwartungshaltung eines Neuwagenkäufer ist beispielsweise die Annahme, dass der Wagen eine Straßenverkehrszulassung besitzt, mängelfrei und fahrtüchtig ist. Explizite sind über schriftliche Verträge, Absprachen und Service-Vereinbarungen dokumentiert.

Die folgenden Abschnitte geben sicherheitsrelevante Gesetze, Grundsätze, Verordnungen, Vorschriften, Ausführungsrichtlinien, Normen und Standards an. Um den Umfang überschaubar zu halten, konzentriere ich mich vorrangig auf deutsche Beispiele. Um den Rahmen dieses Buchs einzuhalten, beschränke ich mich insgesamt auf sehr wenige beispielhaften Auszüge, die mir aufgrund meiner bisherigen Erfahrung, aber als juristischer Laie, wichtig erscheinen. Über das Folgende hinausgehende Informationen finden Sie im „Handbuch Unternehmenssicherheit“ des Autors.

Im Hinblick auf Sorgfalt und Haftung der Geschäftsführung ergeben sich in Deutschland gesetzliche Anforderungen beispielsweise aus dem GmbH-Gesetz und dem Aktiengesetz (AktG). Auf Schadensersatz wegen Pflichtverletzung geht das Bürgerliche Gesetzbuch (BGB), Stand 19.2.2007 in §280 ein.

Haftungsrisiken

Für Chief Executive Officers (CEOs) und Chief Financial Officers (CFOs) von Gesellschaften, die in den USA börsennotiert sind, ergeben sich durch den Sarbanes-Oxley Act (SOX) zusätzliche Risiken. Die dortige Section 302 fordert die eidesstattliche Beglaubigung von Quartals- und Jahresausweisen durch die CEOs und CFOs sowie deren Verantwortlichkeit für Errichtung und Durchführung des internen Kontrollsystems [19].

*Sarbanes-Oxley
Act*

Gemäß Section 302 müssen CEO (principal executive officer or officers) und CFO (principal financial officer or officers) in jedem Quartals- und Jahresbericht bestätigen, dass er von ihnen geprüft wurde, keine unwahren Aussagen enthält und in jeder Hinsicht die finanzielle Situation und das operative Ergebnis für den Berichtszeitraum angemessen darstellt. Ferner bestätigen die Unterzeichner des Berichts, dass sie für Aufbau und Pflege der internen Kontrollen verantwortlich sind, die Effektivität der internen Kontrollen innerhalb von 90 Tagen vor dem Bericht evaluiert haben und ihre Schlüsse über die Effektivität ihrer internen Kontrollen zum Zeitpunkt dieser Evaluation dargestellt haben. Doch was hat dies alles mit der ITK zu tun?

Da die ITK die Daten für die Quartals- und Jahresberichte verarbeitet, muss dort sichergestellt sein, dass die SOX-relevanten ITK-Systeme und Daten identifiziert sind. Ihr Einfluss auf das Berichtswesen, der beispielsweise im Rahmen einer Geschäftseinflussanalyse erhoben

*Sarbanes-Oxley
Act und die ITK*

wird, muss ebenso wie potenzielle Bedrohungen und die damit verbundenen Risiken bekannt sein. Dementsprechend sind für die relevanten Konten Kontrollen zu identifizieren und zu dokumentieren. Laut COBIT® sind hierfür Kontrollen auf Unternehmensebene sowie anwendungsspezifische Kontrollen (Application Controls) und allgemeine IT-Kontrollen (General IT Controls) erforderlich.

Anwendungsspezifische Kontrollen beinhalten beispielsweise die Prüfung der Vollständigkeit und Richtigkeit sowie der angemessenen Funktionstrennung. Beispiele hierfür sind geeignete Kompetenzregelungen und Limite sowie deren Überwachung und die Konsolidierung von Daten.

Allgemeine IT-Kontrollen beziehen sich z. B. auf die Programmentwicklung, den ITK-Betrieb und das Änderungsmanagement. Beispiele hierfür sind u. a. Datenklassifizierung sowie Zutritts-, Zugangs- und Zugriffskontrollen (s. a. Sicherheitsschalenmodell nach Dr.-Ing. Müller). Ebenfalls dazu gehört ein sicherer und kontrollierter Lebenszyklus, wie Sie ihn auch in der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller finden, von der Beantragung, Planung, Spezifikation, Beschaffung und Entwicklung von ITK-Systemen, über deren Test, Installation und Inbetriebnahme bis hin zur Produktion einschließlich der begleitenden Prozesse, wie z. B. des Ereignis-, Problem- und Änderungsmanagements. Neben der Integrität der Daten im Sinne von Vollständigkeit, Konsistenz, Korrektheit und Aktualität ist auch die Verfügbarkeit der Daten relevant, um wesentliche Veränderungen umgehend berichten zu können (real-time reporting).

EuroSOX

Am 17. Mai 2006 verabschiedeten das europäische Parlament und der Rat die Richtlinie 2006/43/EG über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen. Diese Richtlinie heißt in Fachkreisen kurz EuroSOX. Eine der grundlegenden Erwägungen im dortigen Abschnitt 24 ist, dass „Prüfungsausschüsse und ein wirksames internes Kontrollsystem“ einen Beitrag dazu leisten, „finanzielle und betriebliche Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmaß zu begrenzen und die Qualität der Rechnungslegung zu verbessern.“ Die Funktionen, die dem Prüfungsausschuss zugewiesen sind, können demzufolge der Verwaltungs- oder Aufsichtsrat als Ganzes ausüben.

Ausgehend u. a. von diesen Überlegungen sieht die Richtlinie in Artikel 41 vor, dass jedes Unternehmen von öffentlichem Interesse einen Prüfungsausschuss benötigt. Zu den Aufgaben des Prüfungsausschusses gehört u. a. die Überwachung des Rechnungslegungsprozesses, des internen Kontrollsystems und gegebenenfalls des internen Revisionssystems sowie des Risikomanagementsystems bis hin zur

Überwachung des Jahresabschlusses. Um diese Aufgabe wahrnehmen zu können, muss es derartige Prozesse und Systeme im Unternehmen geben.

Deutschen Unternehmen sind Risikomanagementsysteme und Interne Kontrollsysteme aufgrund gesetzlicher Vorgaben nicht fremd. Die teilweisen Parallelen zwischen SOX und dieser EU-Richtlinie, z. B. im Hinblick auf die korrekte Rechnungslegung bzw. Finanzberichtserstattung, haben zur Bezeichnung EuroSOX geführt. In den Auswirkungen auf die ITK gelten die zuvor gemachten Ausführungen zum SOX in entsprechender Form.

Weitere gesetzliche Anforderungen ergeben sich aus dem Bürgerlichen Gesetzbuch (BGB) im Hinblick auf Verträge und dem Handelsgesetzbuch (HGB) hinsichtlich ordnungsmäßiger Buchführung. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), dessen Anforderungen in das AktG und HGB eingeflossen sind, stellt Anforderungen an das Überwachungs-, d. h. Risikomanagementsystem.

*Gesetzliche
Anforderungen*

Wesentliche und auch für die IT relevante Anforderungen an die Buchführung ergeben sich aus dem deutschen Handelsgesetzbuch (HGB), Stand 5. Januar 2007. Hierzu gehören u. a. die **Grundsätze ordnungsmäßiger Buchführung**, die **vollständig, richtig, zeitgerecht und geordnet** vorgenommenen Eintragungen und Aufzeichnungen sowie die Verfügbarkeit der **Daten während der Dauer der Aufbewahrungsfrist** bei der Führung der Handelsbücher auf Datenträgern.

*Handelsgesetz-
buch*

Die Abgabenordnung (AO), Stand 13.12.2006, fordert gemäß § 147 Abs. 2, Ziffer 2, dass „die Daten [...] während der Dauer der Aufbewahrungsfrist **jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet** werden können“.

*Abgaben-
ordnung*

Diese Forderungen aus HGB und AO finden ihren Niederschlag in den Grundsätzen ordnungsmäßiger Buchführung (GoB), ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) sowie für eine ordnungsmäßige Datenverarbeitung (GoDV). Darüber hinaus sind seit dem 1. Januar 2002 die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) des Bundesfinanzministeriums in Kraft.

*GoB, GoBS,
GoDV, GDPdU*

Die GoBS, Stand 7. November 1995, fordert ein Internes Kontrollsystem (IKS). Das IKS muss u. a. die Programmidentität sicherstellen, d. h., dass die eingesetzte DV-Buchführung dem dokumentierten System entspricht. Dies erfordert Richtlinien für Programmierung, Programmtests, -freigaben und -änderungen, für die Änderung von Stamm- und Tabellendaten, für Zugriffs- und Zugangsverfahren, für

*Internes
Kontrollsystem*

den ordnungsgemäßen Einsatz von Datenbanken, Betriebssystemen und Netzwerken sowie den Einsatz von Testdatenbeständen/-systemen und Programmeinsatzkontrollen.

Sicherheitsanforderungen

Laut Anlage zur GoBS, Stand 7. November 1995, Kap. 5.5.2, umfasst die Sicherung der Informationen vor Verlust „die Maßnahmen, durch die für die gesicherten Programme/Datenbestände die Risiken hinsichtlich Unauffindbarkeit, Vernichtung und Diebstahl im erforderlichen Maß reduziert werden.“

Zur Wiederauffindbarkeit sind demzufolge systematische Verzeichnisse der gesicherten Programme und Datenbestände zu führen. Zum Schutz vor Vernichtung sind für die Aufbewahrungsstandorte Bedingungen zu schaffen, die eine Vernichtung bzw. Beeinträchtigung der Informationen durch Feuer, Temperatur, Feuchtigkeit und Magnetfelder etc. weitestgehend ausschließen. Der Bedrohung des Datenträgerdiebstahls ist dadurch zu begegnen, dass die Datenträger in Tresoren aufbewahrt werden, oder in Räumen, die ausreichend gegen Einbruch gesichert sind. Die Überprüfung der Lesbarkeit der Datenträger ist in angemessenen Zeitabständen erforderlich.

Die Anlage zur GoBS fordert weiterhin ein dokumentiertes Datensicherungskonzept. Um die buchhalterisch relevanten Informationen während der Dauer der Aufbewahrungsfrist jederzeit lesbar machen zu können, umfasst das Datensicherungskonzept **die Sicherung der Daten und Software und gegebenenfalls auch der Hardware**.

Aufbewahrungsfristen

Im Kapitel Aufbewahrungsfristen führt die GoBS aus, dass „Daten mit Belegfunktion grundsätzlich sechs Jahre, Daten und sonst erforderliche Aufzeichnungen mit Grundbuch- oder Kontenfunktion [...] grundsätzlich zehn Jahre aufzubewahren“ sind. Wichtig in diesem Zusammenhang erscheint mir, dass die „**Verfahrensdokumentation zur DV-Buchführung** [...] zu den Arbeitsanweisungen und sonstigen Organisationsunterlagen im Sinne des § 257 Abs. 1 HGB bzw. § 147 Abs. 1 AO“ gehört und „grundsätzlich **zehn Jahre aufzubewahren**“ ist.

Anforderungen der Wirtschaftsprüfer an die Informations-technologie

Die deutschen Wirtschaftsprüfer haben sich vielfältige Standards für ihre Prüfungen geschaffen. Zur Prüfung der Informationstechnologie hat das Institut der Wirtschaftsprüfer (IDW) beispielsweise die RS FAIT 1, die RS FAIT 2 und die RS FAIT 3 des Fachausschusses für Informationstechnologie (FAIT) sowie die PS 330, PH 9.330.1 und PS 880 herausgegeben [20], [21].

FAIT 1

IDW RS FAIT 1, (3), konkretisiert die Anforderungen, die aus §§238, 239 und 257 HGB resultieren, für die Führung der Handelsbücher mittels IT-gestützter Systeme [20]. Doch welche Sicherheitsanforde-

rungen ergeben sich hieraus? FAIT 1 führt u. a. aus, dass Maßnahmen zur Vertraulichkeit z. B. Verschlüsselungstechniken sind. Organisatorische Maßnahmen zur Integrität von IT-Systemen sind geeignete Test- und Freigabeverfahren, technische Maßnahmen sind z. B. Firewalls und Virens Scanner. Im Hinblick auf Verfügbarkeit sind beispielsweise geeignete Back-up-Verfahren zur Notfallvorsorge einzurichten und Datensicherungen durchzuführen. Klar definiert sein müssen die Aufgaben, Kompetenzen und Verantwortlichkeiten der IT-Mitarbeiter. Das Verfahren zur Vergabe, Änderung, Entziehung und Sperrung von Berechtigungen sowie deren Protokollierung sind festzulegen.

In Absatz (53) und (54) fordert FAIT 1 für die Nachvollziehbarkeit des Buchführungs- und Rechnungslegungsverfahrens eine ordnungsgemäße Verfahrensbeschreibung, bestehend aus Anwender-, Betriebs- und technischer Systemdokumentation. Laut FAIT 2, Absatz (38), sind Schwerpunkte der Verfahrensdokumentation für E-Commerce die Beschreibungen der eingesetzten Hard- und Software, der verwendeten Protokolle und der Schnittstellen sowie Datenflusspläne und die Darstellung der Netzwerkarchitektur.

Laut FAIT 1, (88), sind Vorkehrungen für einen **Notbetrieb** zu treffen. Weiter wird dort ausgeführt, dass **ein Ausfall wesentlicher IT-Anwendungen** ohne kurzfristige Ausweichmöglichkeit **einen wesentlichen Mangel der Buchführung darstellt**.

Notbetrieb

Die RS FAIT 2 „[...] verdeutlicht [...] die in IDW RS FAIT 1 dargestellten Ordnungsmäßigkeits- und Sicherheitsanforderungen im Bereich von E-Commerce [...]“ [20]. Sie geht insbesondere auch auf die IT-Risiken und die Kriterien zur Beurteilung der Sicherheit und Ordnungsmäßigkeit beim Einsatz von E-Commerce-Systemen ein. Sie fordert hinsichtlich der Dokumentation u. a. **Beschreibungen der eingesetzten Hard- und Software, der Netzwerkarchitektur, der verwendeten Protokolle und Verschlüsselungsverfahren sowie Datenflusspläne**. U. a. geht IDW RS FAIT 1 auch auf die **Aufbewahrungspflichten** ein.

*FAIT 2:
E-Commerce*

RS FAIT 3 [21] konkretisiert die Anforderungen an die Archivierung jener aufbewahrungspflichtigen Unterlagen, die sich aus §257 HGB ergeben. FAIT 3 verdeutlicht die in IDW RS FAIT 1, Tz. 60ff. „dargestellten Aufbewahrungspflichten bei Einsatz von elektronischen Archivierungssystemen“ [...]. Zu den hier angeführten Sicherheitsanforderungen gehören beispielsweise Zugriffskontrollen für Speichermedien und während der gesamten Aufbewahrungsfrist die Verfügbarkeit auch von IT-Anwendungen und IT-Infrastruktur, mit denen die Lesbarmachung möglich ist.

*FAIT 3:
Elektronische
Archivierung*

<i>PS 880: Software- bescheinigung</i>	Der IDW-Prüfungsstandards PS 880 „Erteilung und Verwendung von Softwarebescheinigungen“, Stand: 25.06.1999, spezifiziert die produkt- und systemorientierte Prüfung sowie die Zertifizierung eines Software-Produktes im Hinblick auf Einhaltung der GoB bzw. GoBS unter Beachtung von FAIT 1 und FAIT 2.
<i>Datenschutz- gesetze und Richtlinien</i>	Die Anforderungen an den Datenschutz sind in Deutschland festgelegt im Bundesdatenschutzgesetz (BDSG) und in den Landesdatenschutzgesetzen (LDSG) sowie zum Schutz der Sozialdaten im Sozialgesetzbuch (SGB X). Weitere datenschutzrechtliche Anforderungen stellt das Teledienstedatenschutzgesetz (TDDSG).
<i>Datenschutz Österreich, Schweiz</i>	In Österreich sind Datenschutzanforderungen im Datenschutzgesetz 2000 (DSG 2000) niedergelegt, in der Schweiz im Datenschutzgesetz (DSG) und in der Datenschutzverordnung (VDSG).
<i>Datenschutz EU</i>	Auf EU-Ebene existiert die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
<i>Datenschutz USA</i>	Die USA verwenden im Datenschutz „einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert“, wie es in der Entscheidung der Kommission der Europäischen Gemeinschaft vom 26. Juli 2000 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ gewährleisteten Schutzes heißt. Dementsprechend existieren in den USA verschiedene Datenschutzgesetze (Privacy Act, Privacy Protection Act). Zu den Datenschutzgesetzen bzw. Gesetzen mit datenschutzrelevanten Anforderungen gehören der Children's Online Privacy Protection Act (COPPA), der Electronic Communications Privacy Act, der Gramm-Leach-Bliley Act (GLBA) mit den Ausführungen der Federal Trade Commission (FTC) in den „Standards for Safeguarding Customer Information“, 16 CFR 314, der Privacy Act und der Social Security Act.
<i>Branchen- spezifische Anforderungen</i>	In den verschiedenen Branchen existieren darüber hinaus spezifische Vorgaben, aus denen sich ebenfalls Anforderungen an die ITK ergeben. Bei Banken sind dies z. B. die Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin, deren Anforderungen beim Outsourcing, sowie Basel II des Baseler Ausschusses für Bankenaufsicht. Zur Ausgestaltung von IT-Systemen im Hinblick auf die MaRisk verweist die BaFin auf das IT-Grundschutzhandbuch des BSI sowie die ISO 17799. Nicht als Beispiele angeführt sind die weiteren in diesem Buch genannten internationalen Standards und Practices bzw. die wegweisende, durchgängige und normenübergreifende

Vorgehensweise anhand der dreidimensionalen Sicherheitspyramide des Autors. Im chemischen und pharmazeutischen Bereich existiert die Gute Laborpraxis (Good Laboratory Practice {GLP}) und die Good Manufacturing Practice (GMP) sowie die Good Automated Manufacturing Practice (GAMP) und das Good Electronic Records Management (GERM).

Wenn sich ein Unternehmen im IT-Bereich an branchenübergreifenden (de-facto-)Standards, Normen und Good bzw. Best Practices orientiert, so sind diese ebenfalls zu berücksichtigen, z. B. DIN EN ISO 9001, ISO/IEC 13335, ISO/IEC 17799, ISO/IEC 18028, ISO/IEC 27000-Reihe, IT-GSK und Standards des BSI, ITIL®, die Information Security Governance des IT Governance Institute® und COBIT®. Doch wie lässt sich dies alles zusammenführen?

*IT-Standards,
Normen,
Good und
Best Practices*

Durch die dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller. Sie ist ein durchgängiges und integratives Vorgehensmodell für das Sicherheits-, Kontinuitäts- und Risikomanagement. Sie enthält eine Vielzahl von Sicherheitsaspekten und -elementen, die sich zum Teil und sowohl mehr oder weniger vollständig als auch mehr oder weniger detailliert auch in verschiedenen Normen und Practices finden, und geht über sie hinaus: Gesetzliche, aufsichtliche und normative Elemente finden sich in der Sicherheits-, Kontinuitäts- und Risikopolitik sowie im Konformitätsmanagement (Compliance Management). Der hierarchische Aufbau zeigt Parallelen zur ISO/IEC 13335. Die Prozessarchitektur ähnelt ITIL®, Version 2, und der ISO/IEC 20000, enthält aber weitere Prozesse und zusätzliche Themen. Die Sicherheitspyramide verfügt über Sicherheitselemente, die auch in der ISO/IEC 17799, den IT-Grundschutzkatalogen des BSI sowie den GxP-Forderungen aus der chemischen und pharmazeutischen Industrie angesprochen werden. Kontrollen und Kennzahlen ermöglichen die Überwachung und Steuerung, ein Aspekt, auf den auch COBIT® eingeht. Der Sicherheitsmanagementprozess des Autors orientiert sich am PDCA-Zyklus, den auch die ISO/IEC 27001 nutzt.

*Sicherheits-
pyramide*

Manch ein Unternehmen möchte noch einen Schritt weiter gehen und nicht nur die IT und auch nicht nur die Sicherheit, sondern das Gesamtunternehmen in einem durchgängigen und integrativen Vorgehensmodell organisieren. Dies bietet die eingangs bereits erwähnte dreidimensionale Unternehmenspyramide nach Dr.-Ing. Müller, die sich nicht zuletzt für IT-Dienstleister eignet. Sie unterstützt auch jene Unternehmen, die entweder ein Zertifikat anstreben, z. B. nach DIN EN ISO 9001 der ISO/IEC 20000, oder einen Prüfungsbericht nach SAS 70, Typ II. Die ACG Automation Consulting Group GmbH nutzt

*Unternehmens-
pyramide*

hierfür im Rahmen ihrer Beratungstätigkeit ein eigenes Tool, das dieses Vorgehen unterstützt.

7.2.3 Geschäftseinflussanalyse (Business Impact Analysis)

Sicherheits-
kriterien

Das vorangegangene Unterkapitel skizzierte auszugsweise die vielfältigen externen Sicherheitsanforderungen. Zu diesen kommen die unternehmensspezifischen Anforderungen hinzu. Nun stellt sich die Frage, wie sich hieraus die konkreten Sicherheitsanforderungen der einzelnen Geschäftsprozesse erheben lassen. Hierzu dient die Schutzbedarfs- bzw. Geschäftseinflussanalyse (Business Impact Analysis {BIA}). Während BIAs oftmals unter dem Aspekt der Verfügbarkeit betrachtet werden, empfehle ich, im Rahmen dieser Analyse die Auswirkungen potenzieller Verletzung folgender Sicherheitskriterien zu betrachten:

Primäre Sicherheitskriterien und Sicherheitsverletzungen:	
Sicherheitskriterium	Sicherheitsverletzung
Konformität	Gesetzes-/Normenverstöße
Robustheit	Fehlfunktion durch Fehlbedienung oder technische Fehler
Verfügbarkeit	Unterbrechung, Ausfall
Integrität	Verfälschung, Manipulation
Vertraulichkeit	unberechtigte Einsichtnahme
Verbindlichkeit	Unverbindlichkeit
Authentizität	Unechtheit
Sekundäre Sicherheitskriterien und Sicherheitsverletzungen:	
Sicherheitskriterium	Sicherheitsverletzung
Nachvollziehbarkeit	Keine oder unzureichende Ordnungsmäßigkeit
Nachweisbarkeit	Keine oder unzureichende Beweisbarkeit
Erkennungsfähigkeit	Keine oder unzureichende Ereigniserkennung
Alarmierungsfähigkeit	Keine oder zu späte Alarmierung
Abwehrfähigkeit	Keine oder unzureichende Abwehrfähigkeit

Auswirkungen
von
Sicherheits-
verletzungen,
Sicherheits-
klasse

Für jedes Sicherheitskriterium werden die quantitativen und qualitativen Auswirkungen potenzieller Verletzungen von Sicherheitsanforderungen erhoben. Hierbei sollte deren zeitlicher Verlauf berücksichtigt werden. Aus den Folgen lassen sich die konkreten Sicherheitsanforderungen je Sicherheitskriterium ableiten. Diese führen schließlich zur Sicherheitsklassifizierung des Geschäftsprozesses im Hinblick auf das jeweilige Sicherheitskriterium, d. h. die Zuordnung des Prozesses in eine Schutzbedarfsklasse, die auch als Sicherheits- oder Kritikalitätsklasse bezeichnet wird. Wie läuft eine derartige Erhebung im Einzelnen ab?

Die Geschäftseinflussanalyse erfolgt z. B. über fragenkataloggestützte Interviews mit den verantwortlichen Bereichsleitern. Die Fragen beziehen sich auf externe und interne Sicherheitsanforderungen im Hinblick auf jedes primäre und sekundäre Sicherheitskriterium sowie auf die zeitlich gestaffelten Auswirkungen bei Verletzung dieser Anforderungen. Grundlegende Anforderungen ergeben sich z. B. aus relevanten gesetzlichen, aufsichtsbehördlichen oder vergleichbaren Festlegungen, aus Verträgen sowie aus Normen und Standards, aber auch aus Anforderungen des Unternehmens. Beispiele für Anforderungsarten sind die Ordnungsmäßigkeit, die Verfügbarkeit von Prozessen und Ressourcen, der Datenschutz sowie Aufbewahrungsfristen.

Geschäftseinflussanalyse

Aus dem Ziel, potenzielle Auswirkungen von Sicherheitsverletzungen zu begrenzen, ergeben sich die spezifischen Sicherheitsanforderungen.

Aus der Erhebung der sicherheitsrelevanten Prozess- bzw. Betriebsanforderungen ergeben sich konkrete Sicherheitsziele, die sowohl qualitativer als auch quantitativer und damit messbarer Natur sein können. Bezogen auf die Ordnungsmäßigkeit können dies z. B. das Vier-Augen-Prinzip, Funktionstrennung, Vollmachtenregelungen und elektronischer Workflow mit Berechtigungskonzept sein. Im Hinblick auf die Verfügbarkeit sind dies z. B. die Betriebszeit, die maximal tolerierbare Ausfallzeit eines Schutzobjekts, die maximale Anzahl von Ausfällen und die minimale Zeit zwischen zwei Ausfällen.

Prozessanforderungen

Die Geschäftseinflussanalyse schließt ferner die Ermittlung des Mindestgeschäftsbetriebs ein, d. h. mit welcher minimalen „Leistung“ des Geschäftsprozesses kann die Handlungsfähigkeit des Unternehmens im Not- oder Katastrophenfall noch aufrecht erhalten werden. Auch hier ist die zeitliche Perspektive zu berücksichtigen, da der tolerierbare Mindestgeschäftsbetrieb zu Anfang üblicherweise niedriger ist und im Laufe der Zeit wieder zunimmt. Für den Zeitraum des Mindestgeschäftsbetriebs kann der Prozesseigner beispielsweise definieren, mit welcher Priorität der Prozess welche Leistungen erbringt. Die höchste Priorität könnten beispielsweise Aufträge oder Anfragen von A-Kunden haben etc.

Zeitlich gestaffelter Mindestgeschäftsbetrieb

Aus dem maximal tolerierbaren Verlust von Daten und Informationen ergeben sich Sicherungsanforderungen, z. B. welche Daten, Unterlagen und Arbeitsmittel müssen in welchem Rhythmus wie gesichert und wie aufbewahrt werden. Messkriterium hierfür ist der Wiederherstellungszeitpunkt, der auch als Recovery Point Objective (RPO) bezeichnet wird. Der RPO kennzeichnet den Zeitpunkt in der

Sicherungsanforderungen

Vergangenheit, für den die Daten nach einer Störung vollständig und korrekt wieder herstellbar sind. Für korrekte arbeitstägliche Datensicherungen beträgt der Wiederherstellungszeitpunkt dementsprechend einen Arbeitstag. Die Wahl des RPO hängt davon ab, welche Daten, z. B. durch Nacherfassung, wiederhergestellt werden können, welche Kosten dadurch entstehen und wie sich die Nutzung des Schutzobjekts und des Geschäftsprozesses dadurch verzögert.

*Archivierungs-
anforderungen*

Insbesondere von externer Seite bestehen längerfristige Archivierungsanforderungen, z. B. bezüglich der Aufbewahrungsdauer von Buchungsbelegen, Verträgen, Analyseergebnissen und Produktbeschreibungen. Die BIA ermittelt die entsprechenden Aufbewahrungszeiträume.

*Sicherheits-
klassifizierung*

Nachdem die konkreten Sicherheitsanforderungen erhoben worden sind, erfolgt die Klassifizierung der Prozesse. Da einzelne Prozessschritte des jeweiligen Gesamtprozesses einen geringeren Schutzbedarf haben können, z. B. weil sie länger verzichtbar sind, wird dies zusätzlich betrachtet. Die Geschäftseinflussanalyse nimmt die entsprechenden Einstufungen auf. Diese gegebenenfalls niedrigeren Einstufungen führen bei der folgenden Betriebseinflussanalyse zu entsprechend geringeren Anforderungen an das jeweilige Schutzobjekt.

7.2.4 Betriebseinflussanalyse (Operational Impact Analysis)

*Schutzbedarfs-
analyse je
Ressource*

Im nächsten Schritt erfolgt für jedes Schutzobjekt, das für die Funktions- und Handlungsfähigkeit eines Prozesses, eines Prozessschrittes bzw. einer Organisationseinheit erforderlich ist, eine standardisierte Betriebseinflussanalyse (Operational Impact Analysis {OIA}). Ist das Schutzobjekt ein Informationssystem, so wird dies auch als ITK-Schutzbedarfsanalyse bezeichnet. Die OIA umfasst je Schutzobjekt folgende Elemente:

- Bezeichnung des Schutzobjekts, z. B. des Informationssystems, des Gebäudes, des Raums, des Arbeitsmittels oder des Services
- Standort des Schutzobjekts
- Schutzobjektverantwortlicher, Service-Geber, Service-Nehmer
- Verweis auf die Prozesscharakteristika des nutzenden Prozesses und Prozessschrittes (Stammdaten, Schnittstellen, rechtliche Rahmenbedingungen, zeitlich gestaffelter Mindestgeschäftsbetrieb, zeitlich gestaffelte Folgen von Sicherheitsverletzungen, maximal tolerierbare Ausfallzeit, minimaler Abstand zwischen zwei Ausfällen, Sicherheitsanforderungen, Sicherheitsklasse je Sicherheitskriterium)

- Verbindungsstellen (Schnittstellen) zu anderen Prozessschritten und Schutzobjekten, wie z. B. Anwendungen, Plattformen, Datenbanken, Ein-/Ausgabemedien
- genutzte Ressourcen (Schutzobjekte) und deren Ausprägung, wie z. B. Kapazität, Anzahl und Qualifikationsprofil der Mitarbeiter, Lokation, Größe und Anzahl der Räumlichkeiten und deren Infrastruktur, Ausstattung der Arbeitsplätze, genutzte Arbeitsmittel, Informationssysteme und Services
- Nutzungsinformationen, z. B. Anzahl der Nutzer, Zeitpunkt bzw. Zeitraum der Nutzung sowie Nutzungsintensität, Datenvolumina und Prognose der Nutzung
- Sicherheitsrelevante Prozess- bzw. Betriebsanforderungen
- Monitoring (welches System stellt welche Informationen auf Basis welcher Informationsquellen in welcher Form und welcher Qualität für wen wo bereit)
- Berichtswesen (wer stellt wann welche Informationen auf Basis welcher Informationsquellen in welcher Form und welcher Qualität für wen wo bereit)
- zeitlich gestaffelte quantifizierte Folgen von Sicherheitsverletzungen anhand konkreter Schadensszenarien, z. B. im Hinblick auf die Unversehrtheit von Menschen, die Aufgabenerfüllung, Handlungsfähigkeit, Finanzen, Strafen, Wettbewerbsfähigkeit, Unternehmensstrategie, Nacharbeit und Restaurierbarkeit sowie das Image
- zeitlich gestaffelter Mindestbetrieb
- Sicherheitsanforderungen je Sicherheitskriterium
- Sicherheitsklasse je Sicherheitskriterium
- Wiederanlaufzeit
- weitere Informationen.

7.3 Tabelle Schadensszenarien

In der folgenden Tabelle sind auszugsweise Beispiele zu Auswirkungen von Bedrohungen in Form von Schadensszenarien für die Schutzobjektklasse Informationssysteme angegeben, die bei der Ermittlung der Folgen von Sicherheitsverletzungen nützlich sind. Aus Platzgründen wurden die rechts liegenden Zeilen in der Folge zusammengefasst, müssen jedoch stets vollständig berücksichtigt werden.

Szenario	Folge	nach ...					Bemerkung
		1h	4h	24h	48h	120h	
Welche Folgen hat ...							
... der Ausfall des Informationssystems?	M						
	A						
	H						
	F						
	I						
	S						
	W						
	U						
	N						
... eine Fehlfunktion des Informationssystems?	s. o.						
	...						
... eine Fehlbedienung des Informationssystems?	s. o.						
	...						
... eine Datenverfälschung durch Manipulation?	s. o.						
	...						
... eine Datenverfälschung durch technische Fehler?	s. o.						
	...						
... die Einsichtnahme Unberechtigter in vertrauliche Daten, z. B. Unternehmensstrategie, Forschungsergebnisse, neue Produkte?	s. o.						
	...						
... die Einsichtnahme Unberechtigter in vertrauliche Daten, z. B. personenbezogene Daten z. B. aufgrund nicht vertraulich vernichteter Datenträger?	s. o.						
	...						
... die Veröffentlichung personenbezogener Daten, z. B. aufgrund nicht vertraulich vernichteter Datenträger?	s. o.						
	...						
... „unechte“ Daten, z. B. durch Vorspiegelung einer falschen Identität?	s. o.						
	...						
...	s. o.						
	...						
Legende:	I = Image S = Strafen W = Wettbewerbsfähigkeit U = Unternehmensstrategie N = Nacharbeit und Restaurierbarkeit						
M = Unversehrtheit von Menschen							
A = Aufgabenerfüllung							
H = Handlungsfähigkeit							
F = Finanzen							

7.4 Praxisbeispiele

Die folgenden Beispiele zeigen, wie der Schutzbedarf von Prozessen und ITK-Systemen erhoben bzw. dargestellt werden kann.

7.4.1 Schutzbedarf der Geschäftsprozesse

Die Ergebnisse der Erhebung und Klassifizierung der Prozesse mit ihren Abhängigkeiten von Schutzobjekten im Rahmen einer Schutzbedarfsanalyse lassen sich je Schutzobjekt überblicksartig darstellen. Die folgende Tabelle zeigt dies prinzipiell, auszugsweise und beispielhaft für das Schutzobjekt Informationssysteme.

Prozess	Unterstützende ITK-Systeme			Sonstiges
	ITK-System 1	ITK-System ...	ITK-System n	
Prozess A	V1, I1, T1, A1	/	/	
...	...	...	...	...
Prozess M	/	/	V4, I2, T2, A3	

Legende:

/ = Informationssystem unterstützt den Geschäftsprozess nicht

V1 ... V4 = Verfügbarkeitsklassen, I1 ... I4 = Integritätsklassen,

T1 ... T4 = Vertraulichkeitsklassen, A1 ... A4 = Verbindlichkeitsklassen

7.4.2 ITK-Schutzbedarfsanalyse

Das folgende Beispiel zeigt das Ergebnisformular einer standardisierten ITK-Schutzbedarfsanalyse.

Ergebnisbeispiel

Stammdaten	
Service-Nehmer:	Beauftragende Organisationseinheit
Ansprechpartner:	Ansprechpartner auf Seiten des Service-Nehmers einschließlich Standort, Telefonnummer(n) und E-Mail-Adresse
Organisationseinheit:	Organisationseinheit, welcher der Ansprechpartner angehört
Service-Geber:	Ausführende Organisationseinheit
ITK-System:	Bezeichnung und gegebenenfalls Release des ITK-Systems
Inbetriebnahmetermin:	Termin, zu dem das ITK-System in Betrieb geht
Geschäftsprozess(e):	Geschäftsprozess(e), der/die durch das ITK-System unterstützt wird/werden
Geschäftsprozessschritt(e):	Geschäftsprozessschritt(e), der/die durch das ITK-System unterstützt wird/werden

Schnittstellen		
Schnittstellenbezeichnung und -typ sowie Anwendung:	Angabe der Schnittstellen zu anderen unternehmensinternen oder –externen Informationssystemen einschließlich des Schnittstellentyps, z. B. Datei, Datenbank, Diskette, ...	
Rechtliche Rahmenbedingungen		
Gesetze, Vorschriften, Normen, Standards und Verträge:	Angabe der Gesetze und Paragraphen, Vorschriften, Normen, Standards oder Verträge, die für das Informationssystem relevant sind. (z. B. AktG, AO, ArbSchG, ASiG, Basel II, BDSG, BGB, BGR, BGV, EuroSOX, FAIT 1, FAIT 2, FAIT 3, GDPdU, GoB, GoBS, GoDV, GwG, HGB, KWG, LDSC, MaRisk, PS 330, SGB VII, SGB X, Solvency II, SOX, TDG, TDDSG, WpHG)	
Systeminformationen		
Standort:	Ort, Straße, Gebäude, Geschoss, Raum	
Rechner:	Bezeichnung des Computersystems, auf dem das ITK-System läuft/laufen soll (Hersteller, Modell, Konfiguration, sowie technische Daten wie z. B. Abmessungen, Stromverbrauch, Abwärme)	
Betriebssystem:	Bezeichnung des Betriebssystems, unter dem das ITK-System läuft/laufen soll	
Datenbank:	Bezeichnung der Datenbank, die das ITK-System nutzt/nutzen soll	
...:		
Nutzungsinformationen		
Anzahl Nutzer:		
Nutzungsintensitätsprofil:	Transaktionsaufkommen über den Tages- und Jahresverlauf, ggf. auch Wochen- und Monatsverlauf	
Nutzergruppenprofil:	Angabe der Rollen, die über welche Funktionen/Transaktionen des Informationssystems mit welchen Rechten (lesen, schreiben, ...) auf welche Daten oder Datenwerte zugreifen dürfen. Bei vielen oder umfangreichen Rollen kann hierzu eine Anlage beigelegt werden.	
	Rolle	Aufgaben Funktion/Transaktion, Daten und Recht
	...	...

Aktuelles Datenvolumen:	Anzahl, Umfang und Art der Datensätze, z. B. Stammdaten, Bewegungsdaten, sowie aktuelles Datenvolumen
Veränderung des Datenvolumens:	Zu-/Abnahme der Anzahl der Datensätze pro Monat und prognostizierte zeitliche Entwicklung des Datenvolumens
Art der Daten:	Personenbezogene Daten
	Sozialdaten
	Unternehmensdaten
	– Vertraulichkeitsgrad
	– - öffentlich (ö), intern (i), vertraulich (v), geheim (g)
Sicherungsintervall:	Zeitpunkte, an denen Datensicherungen durchgeführt werden sollen, z. B. arbeits-täglich einmal, nach 20:00 Uhr. Orientierung gibt hier die Möglichkeit und der Aufwand für die Neuerfassung der Daten bei Verlust.
Letzter wieder herstellbarer Zeitpunkt (maximal tolerierbarer Datenverlust)	Der letzte wieder herstellbare Zeitpunkt gibt an, wie groß der maximale zeitliche Abstand zu jenem System- und Datenzustand sein darf, der z. B. nach einer Rückspeicherung der Daten wiederherstellbar ist.
Sicherungsfenster	Zeitraum, der für die Sicherung zur Verfügung steht mit Angabe des jeweiligen Arbeitstages
Sicherungsdauer	Errechnete und verifizierte Dauer der Datensicherung und prognostizierte zeitliche Steigerung auf Basis des Datenvolumens und dessen prognostizierter Veränderung (mit Input von der ITK)
Sicherungstool	Werkzeug, das zur Datensicherung eingesetzt werden soll (mit Input von der ITK)
Sicherungsmethode	Komplett, differenziell, inkrementell, selektiv (mit Input von der ITK)
Archivierungsanforderungen:	Vorgaben zum Archivierungszeitpunkt und zur Archivierungsdauer, gegebenenfalls Hinweis auf z. B. gesetzliche Anforderungen
Sicherheitsrelevante Betriebsanforderungen	
Betriebszeit:	Tage und Zeitraum, z. B. arbeitstäglich 7:00 – 19:00
Support-Zeit:	Tage und Zeitraum, z. B.

	arbeitstglich 8:00 – 18:00
Antwortzeitverhalten:	Prozentuale Angaben, z. B. bezogen auf Transaktionen: 90 %: <= 1sec, 5 %: 1-2sec, 5 %: 2-5sec
Max. tolerierbare Ausfallzeit:	Angabe der Dauer und des Bezugszeitraums, z. B.: 4h whrend der Betriebszeit
Max. Ausfallzeit pro Jahr:	Angabe der Dauer und des Bezugszeitraums, z. B.: 16h whrend der Betriebszeit
Minimaler Ausfallabstand:	Minimal tragbarer zeitlicher Abstand zwischen zwei Ausfllen, z. B. Arbeitstage
Berichtswesen	
Berichtsrhythmus:	Angabe des Zeitpunkts und zeitlichen Abstands der Berichte, z. B.: Jeweils am 5. Arbeitstag eines Monats
Berichtsinhalte:	Management Summary ber die Erfllung/Nichterfllung der Anforderungen Kurve des Antwortzeitverhaltens mit Grenzeraden je Antwortzeitbereich Tortendiagramm ber den prozentualen Anteil je Antwortzeitbereich Kurve ber Anzahl und Dauer der Ausflle mit Grenzgerade ...
Folgen von Sicherheitsverletzungen je Sicherheitskriterium	
Konformitt	Beschreibung der Folgen und des Ausmaes
Robustheit	Beschreibung der Folgen und des Ausmaes
Verfgbarkeit:	Beschreibung der Folgen und des Ausmaes
Integritt:	Beschreibung der Folgen und des Ausmaes
Vertraulichkeit:	Beschreibung der Folgen und des Ausmaes
Verbindlichkeit:	Beschreibung der Folgen und des Ausmaes
...	
Resultierende Sicherheitsklassen	
Konformitt	Angabe der Konformittsklasse
Robustheit	Angabe der Robustheitsklasse
Verfgbarkeit:	Angabe der Verfgbarkeitsklasse
Integritt:	Angabe der Integrittsklasse
Vertraulichkeit:	Angabe der Vertraulichkeitsklasse
Verbindlichkeit:	Angabe der Verbindlichkeitsklasse
...	
Weitere Informationen	
...	

7.4.3 Schutzbedarfsklassen

Die Schutzbedarfsklassen orientieren sich an den Anforderungen und Möglichkeiten des jeweiligen Unternehmens. Für kleinere Unternehmen sind beispielsweise bereits finanzielle Schäden nicht mehr tragbar, die für ein Großunternehmen unerheblich sind. Daher müssen die in der folgenden auszugsweisen Tabelle beispielhaft angegebenen Folgen unternehmensspezifisch überprüft und quantifiziert werden.

Sicherheitskriterium	
Schutzbedarfsklasse und Folge einer Sicherheitsverletzung	
Verfügbarkeit	
V1	Eine <u>Ausfalldauer</u> von bis zu 5 Arbeitstagen hat keinerlei nennenswerte negative Auswirkungen auf den betroffenen Geschäftsprozess. Die <u>maximale Ausfallzeit</u> pro Jahr darf 10 Arbeitstage nicht überschreiten. <u>Personelle Schäden</u> können nicht auftreten. Der <u>gesamte finanzielle Schaden</u> liegt bei weniger als 1.000 EUR. Auswirkungen auf Image, Strategie, Nacharbeit oder andere Themenbereich sind vernachlässigbar.
V2	Eine <u>Ausfalldauer</u> von bis zu 3 Arbeitstagen kann toleriert werden. Die <u>maximale Ausfallzeit</u> pro Jahr darf 4 Arbeitstage nicht überschreiten. <u>Personelle Schäden</u> können nicht auftreten. Bei Überschreiten der Ausfallzeit können folgende Konsequenzen auftreten: ...
V3	Eine <u>Ausfalldauer</u> von bis zu 1 Arbeitstag kann toleriert werden. Die <u>maximale Ausfallzeit</u> pro Jahr darf 2 Arbeitstage nicht überschreiten. <u>Personelle Schäden</u> können nicht auftreten. Bei Überschreiten der Ausfallzeit können folgende Konsequenzen auftreten: ...
V4	Eine <u>Ausfalldauer</u> von bis zu maximal 4 Stunden kann toleriert werden. Die <u>maximale Ausfallzeit</u> pro Jahr darf 8 Stunden nicht überschreiten. Bei Überschreiten der Ausfallzeit kann eine der folgenden Konsequenzen auftreten: Personenschäden potenzielle finanzielle Schäden von mehr als 1 Mio. EUR nachhaltige Imageschädigung mit potenziellen Umsatzverlusten von mehr als 10 Mio. EUR ...

Vertraulichkeit	
T1	Die Informationen sind öffentlich. Eine Verbreitung hat keinerlei negative Konsequenzen.
T2	Die Informationen sind zur unternehmensinternen Nutzung bestimmt. Eine Verletzung der Vertraulichkeit kann nur geringe negative Folgen nach sich ziehen.
T3	Die Daten sind als vertraulich eingestuft und dürfen nur einem definierten Personenkreis zugänglich sein. Eine Verletzung der Vertraulichkeit kann strafrechtliche, finanzielle oder imagebeeinträchtigende Konsequenzen nach sich ziehen.
T4	Die Daten sind als geheim eingestuft und dürfen nur einem eng begrenzten Personenkreis zugänglich sein. Eine Verletzung der Vertraulichkeit kann für das Unternehmen existenzbedrohend sein. Hierzu zählen beispielsweise geheime Forschungsergebnisse, geheime Strategien etc.
...	

7.5 Zusammenfassung

*Prozess-
architektur*

Ausgangsbasis der ITK-Schutzbedarfsanalyse sind die Kerngeschäfts-, Unterstützungs- und Begleitprozesse des Unternehmens. Sie sind in der Prozessarchitektur dargestellt. Diese enthält neben den Prozessen und deren Zusammenwirken Angaben zur Bedeutung des jeweiligen Prozesses für das Unternehmen. Für jeden Prozess sind die genutzten ITK-Systeme angegeben.

*Schutzbedarfs-
klassen*

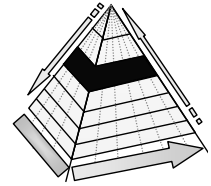
Zur Reduzierung der Komplexität und Steigerung der Effizienz empfiehlt es sich, ähnlich standardisierte Schutzbedarfsklassen zu definieren, wie sie das vorangegangene Beispiel enthält.

*Schutzbedarfs-
analyse*

Der Schutzbedarf von ITK-Systemen wird mittels der ITK-Schutzbedarfsanalyse ermittelt und ähnlich dem vorangegangenen Beispiel dokumentiert. Hierbei werden nicht nur die Folgen von Sicherheitsverletzungen und Ausfällen erhoben, sondern auch die sicherheitsrelevanten Anforderungen, das Mengengerüst und die Benutzerrollen. Die Schutzbedarfsanalyse umfasst die Geschäfts- und die Betriebseinflussanalyse.

8 Sicherheitstransformation

Die Sicherheitsanforderungen eines Unternehmens sind über die Sicherheits-, Kontinuitäts- und Risikopolitik und die Sicherheitsziele bzw. -anforderungen definiert. Die Sicherheitsanforderungen müssen auf die Kerngeschäftsprozesse selbst abgebildet werden sowie auf all jene Ressourcen (z. B. ITK-Systeme), Prozesse, Leistungen (Services) und Produkte, die ein Kerngeschäftsprozess nutzt. Als Ergebnis der Abbildung bzw. Transformation stehen den Anforderungen schließlich entsprechende Sicherheitscharakteristika gegenüber, beispielsweise für die genutzten Ressourcen. Bei der Transformation sind auch Kosten-Nutzen-Aspekte zu berücksichtigen.



Wie lässt sich diese Transformation zielorientiert durchführen? Gemäß [6], [7] und laut DIN EN ISO 8402 von 1995 sowie ISO 9126 ist Sicherheit ein Qualitätsmerkmal. Es liegt daher nahe, für die Abbildung der Sicherheitsanforderungen Methoden zu verwenden, die aus dem Qualitätsmanagement stammen. Dort lassen sich Kundenanforderungen auf Produkt- und Prozessmerkmale transformieren, indem das Quality Function Deployment [22] und das House of Quality [22] genutzt werden.

In vergleichbarer Form kann ein Safety and Security Function Deployment (SSFD) bzw. ein Safety, Security and Continuity Function Deployment (SSCFD) unter Zugrundelegung des House of Safety and Security (HoSS) bzw. des House of Safety, Security and Continuity (HoSSC) durchgeführt werden. Dieser schrittweise methodische Ansatz ist insbesondere für größere Unternehmen und komplexere ITK-Installationen interessant. Wer ein anderes Vorgehen wählt, muss dabei darauf achten, dass der Transformationsvorgang in den Lebenszyklus von Prozessen, Ressourcen, ITK-Systemen, Dienstleistungen und Produkten integriert ist.

Folgende Unterkapitel behandeln dieses Thema:

1. Haus zur Sicherheit – House of Safety, Security and Continuity (HoSSC)
2. Safety, Security and Continuity Function Deployment
3. Schutzbedarfsklassen
4. Praxisbeispiele
5. Zusammenfassung

8.1 Haus zur Sicherheit – House of Safety, Security and Continuity (HoSSC)

Das House of Safety, Security and Continuity hat folgendes Aussehen:

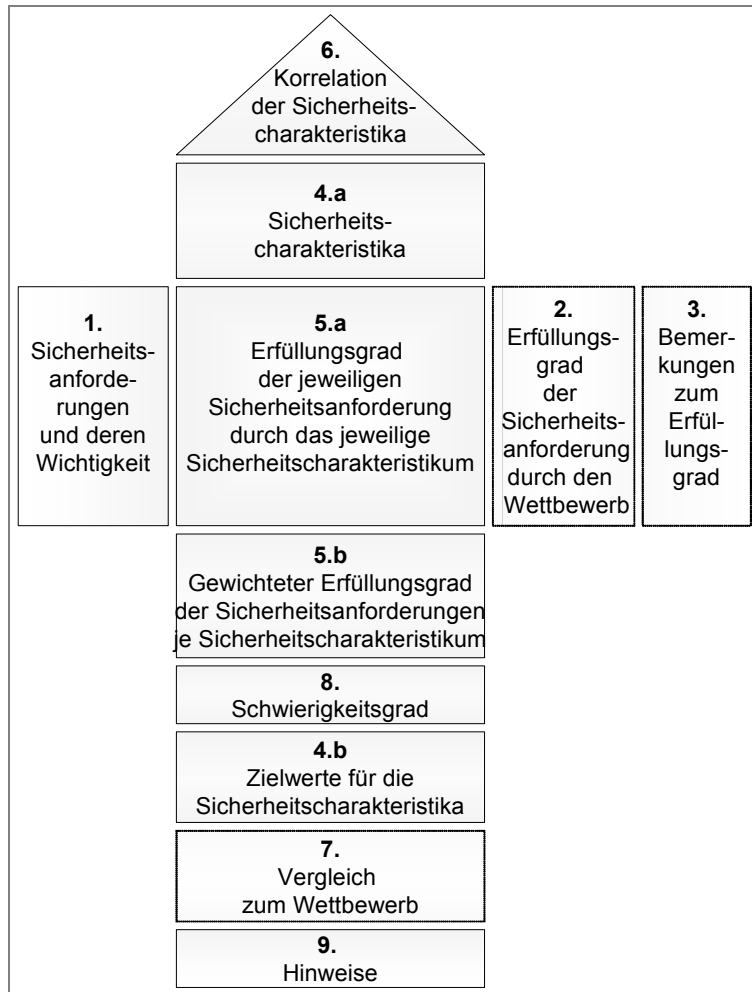


Abb. 8.1: House of Safety, Security and Continuity (HoSSC)

*Ausgangspunkt
und Ziel*

Ausgangspunkt im House of Safety, Security and Continuity (HoSSC) sind die fachlich geprägten Sicherheitsanforderungen (1.) der Nutzer. Ziel ist deren Transformation in entsprechende Sicherheitscharakteristika (4.), der Erfüllungsgrad (5.), mit dem das jeweili-

ge Sicherheitscharakteristikum die Anforderungen erfüllt und die gegenseitige Beeinflussung (6.) der Sicherheitscharakteristika untereinander. Die Transformation wandelt also das „was“ gefordert ist in ein „wie“, d. h. durch welche Sicherheitscharakteristika es zu realisieren ist, um.

Bei der Anwendung des HoSSC ist zu berücksichtigen, dass es sich mit der Transformation „nur“ der Sicherheitsanforderungen auf Sicherheitscharakteristika befasst. Wenngleich Sicherheit hier im Sinne von Betriebs- und Angriffssicherheit sowie Kontinuität zu verstehen ist, geraten hierdurch andere Aspekte des gesamten Anforderungsspektrums in den Hintergrund. Daher ist sicherzustellen, dass die Sicherheitscharakteristika mit anderen Anforderungen hinreichend verträglich sind. Beispielsweise kann ein sehr sicher konzipiertes System dazu führen, dass seine Nutzbarkeit im Hinblick auf das Antwortzeitverhalten reduziert wird, oder umfangreiche zusätzliche organisatorische Maßnahmen den Nutzen des Systems in Frage stellen. Daher empfiehlt es sich, diese Aspekte nach und nach mit zu berücksichtigen.

Anforderungsspektrum

8.2 Safety, Security and Continuity Function Deployment (SSCFD)

Die Transformation der Sicherheitsanforderungen, das Safety, Security and Continuity Function Deployment, erfolgt – ausgehend vom Haus zur Sicherheit – in folgenden Schritten:

1. Transformation der Anforderungen auf Sicherheitscharakteristika
2. Detaillierung der Sicherheitscharakteristika
3. Abbildung der Sicherheitscharakteristika auf Prozesse und Lebenszyklen.

8.2.1 Transformation der Anforderungen auf Sicherheitscharakteristika

Der Transformationsvorgang der fachlich geprägten Sicherheitsanforderungen der Nutzer in Sicherheitscharakteristika erfolgt über die Elemente des House of Safety, Security and Continuity.

Transformationsvorgang

Ausgangspunkt sind die Sicherheitsanforderungen (1.) und ihre Wichtigkeit. Bei der Wichtigkeitseinstufung können gegebenenfalls auch die Folgen von Sicherheitsverletzungen und die Eintrittswahrscheinlichkeit von Bedrohungen betrachtet werden. Da sich die Eintrittswahrscheinlichkeiten von Bedrohungen, z. B. durch Stürme oder Hochwasser,

Ausgangspunkt Sicherheitsanforderungen

kurzfristig ändern können, und die Wahrscheinlichkeit nichts darüber aussagt, ob diese Bedrohungen nicht vielleicht schon morgen eintreten, ist hier Vorsicht angebracht. Für unternehmenskritische Szenarien kann es sich durchaus empfehlen, bestimmte Bedrohungen als „sicher vorhanden“, d. h. mit der Eintrittswahrscheinlichkeit 1, anzunehmen. Hierdurch vermeiden Sie, dass diese Bedrohungen und damit die Sicherheitsanforderungen durch die Gewichtung so in den Hintergrund treten, dass ein Eintreten der Bedrohung das Unternehmen vernichtet.

Optional lässt sich in das Haus zur Sicherheit eintragen, inwieweit Sicherheitsanforderungen derzeit im Vergleich zum Wettbewerb erfüllt werden (2.). Dies spielt bei Entscheidungen auf Managementebene oftmals eine wesentliche Rolle. Zusätzlich können Bemerkungen dokumentiert werden, die z. B. Quellen oder Gründe für diese Bewertung angeben.

*Transformation
in Sicherheits-
charakteristika*

Die Transformation der Sicherheitsanforderungen erfolgt, indem Sicherheitscharakteristika (4.a) angegeben werden, mittels derer die Sicherheitsanforderungen erfüllt werden können. Die Sicherheitscharakteristika werden in Gruppen zusammengefasst. Diese orientieren sich einerseits daran, welchem Themenfeld von PROSim sie zugeordnet sind und andererseits, welchen Zweck sie verfolgen, nämlich vorbeugend, beobachtend, erkennend, meldend, erwidern, (schadens-)beurteilend, wiederherstellend und verbessernd. Dies macht unvollständig transformierte Anforderungen sichtbar.

Die Anforderung nach höchster Geheimhaltung führt z. B. zu einem eng begrenzten Nutzerkreis, Rechteverwaltung, Zufahrts-, Zutritts-, Zugangs-, Zugriffs- und Leseschutz, Wiederaufbereitung von Datenträgern, Absendekontrolle, Übertragungssicherung, Alarmierung, Protokollierung und Protokollauswertung.

Zielwerte

Für jedes Sicherheitscharakteristikum wird darüber hinaus festgelegt, welcher Zielwert erreicht werden muss (4.b).

So führt die Kundenanforderung nach einer maximalen Ausfalldauer von 1h pro Jahr zum Sicherheitscharakteristikum „Verfügbarkeit 99,99 %“. Die Anforderung nach höchster Geheimhaltung beschränkt den Zugriff für derartige Dokumente und Daten auf einen kleinen Leserkreis, z. B. auf die Geschäftsleitung.

*Bewertung der
Sicherheits-
charakteristika*

Der nächste Schritt (5.a) bewertet, wie stark das jeweilige Sicherheitscharakteristikum welche Sicherheitsanforderung unterstützt. Nach diesen Einzelbewertungen wird je Feld das Produkt aus Wichtigkeit der Sicherheitsanforderung und Erfüllungsgrad des Sicherheitscharakteristikums errechnet. Die Summe dieser Werte (5.b) je Charakte-

ristikum gibt an, wie stark das jeweilige Sicherheitscharakteristikum alle Sicherheitsanforderungen erfüllt.

Die Sicherheitscharakteristika können sich gegenseitig mehr oder weniger stark positiv oder negativ beeinflussen. Diese Korrelation zueinander spiegelt sich im Dach des HoSSC (6.) wider.

*Korrelation der
Sicherheits-
charakteristika*

Die Bewertung der Sicherheitscharakteristika im Vergleich zum Wettbewerb lässt sich ebenfalls erfassen (7.). Angaben zum Schwierigkeitsgrad der Realisierung (8.) und Kommentare bzw. Hinweise (9.) zu den Sicherheitscharakteristika vervollständigen das HoSSC.

*Vergleich zum
Wettbewerb*

Als Ergebnis sind die Sicherheitscharakteristika identifiziert und bewertet. Die Detaillierung der kritischen und wichtigen Sicherheitscharakteristika erfolgt in der nächsten Phase.

Ergebnis

8.2.2 Detaillierung der Sicherheitscharakteristika

Die ermittelten kritischen und wichtigen Sicherheitscharakteristika des vorangegangenen Schrittes müssen für ihre spätere Umsetzung weiter detailliert bzw. konkretisiert werden. Hierzu werden sie mit ihrer Gewichtung als Anforderungen in einem weiteren „abgespeckten“ HoSSC (1., 5.a, 4.a, 4.b) aufgelistet und mit den erhobenen Zielwerten versehen. Zusätzlich werden Maßnahmen aufgenommen, die zwar nicht explizit gefordert, aber implizit erwartet werden.

Beispielsweise kann eine geforderte Verfügbarkeit von 99,99 % umgesetzt werden durch u. a. zwei hochverfügbare Rechnersysteme in zwei Rechenzentren an 10km voneinander entfernt liegenden Standorten und eine synchrone standortübergreifende Plattenspiegelung.

8.2.3 Abbildung der Charakteristika auf den Lebenszyklus

Zur Umsetzung der ermittelten Sicherheitscharakteristika sind jedoch oftmals entsprechende Prozesse erforderlich. Z. B. zieht die Anforderung nach einer unterbrechungsfreien Stromversorgung nach sich, dass diese geplant, beschafft, installiert, betrieben, gewartet und irgendwann einmal ersetzt werden muss. Ähnlich verhält es sich bei Informationssystemen. Auch hier müssen die Anwendungen, Rechner, Plattenspeicher, Ein- und Ausgabemedien, Netze, etc. geplant, beschafft oder entwickelt, aufgebaut, betrieben und später außer Betrieb genommen werden.

Diese Beispiele, die sich verallgemeinern lassen, zeigen, dass eine weitere Abbildung erforderlich ist. Hierzu werden aus den zuvor näher spezifizierten Sicherheitscharakteristika entsprechende (sicherheitsrelevante) Anforderungen für den Lebenszyklus z. B. eines Systems entwickelt. Dieser erstreckt sich von der ersten Idee über die

Planung, Beschaffung, Entwicklung, Prüfung, den Test, die Inbetriebnahme und den Betrieb bis hin zur Außerbetriebnahme. Den Lebenszyklus begleiten weitere Prozesse, wie z. B. das Leistungs-, Änderungs-, Konfigurations-, Problem-, Datenschutz-, Sicherheits- und Kontinuitätsmanagement, für die ebenfalls sicherheitsrelevante Anforderungen abgeleitet werden. Auch hier lässt sich wieder ein „abgespecktes“ HoSSC nutzen.

Beispiel

Führte beispielsweise die Anforderung nach einem hochverfügbaren Informationssystem zum Einsatz doppelter Rechnersysteme, Plattenspiegelung und zwei infrastrukturell abgesicherten Standorten, so hat dies zu einem Auswirkung auf den Lebenszyklus des Informationssystems: Diese Anforderungen fließen dort u. a. in die Kosten-Nutzen-Betrachtung, die technische Spezifikation, die Entwicklung und den Test ein. Zum anderen folgen hieraus Anforderungen an die IT-Prozesse, die z. B. beim Systems- und Netzmanagement sowie dem Kapazitäts- und Kontinuitätsmanagement der ITK-Systeme zu berücksichtigen sind.

Weitere Auswirkungen ergeben sich auf das Facility Management, da jetzt zwei Standorte zu betreuen, mit der erforderlichen Haustechnik zu versehen und zu betreiben sind. Aufgrund der infrastrukturellen Absicherung, z. B. durch eine Netzersatzanlage, beinhaltet der Betriebsprozess daher, dass diese zu warten und regelmäßig nachvollziehbar auf Funktionsfähigkeit zu prüfen ist.

Klassifizierung der Prozesse

Für die Prozesse und Begleitprozesse, beispielsweise in der IT und im Facility Management, führt dies zu Sicherheitsanforderungen. Die Erhebung der Sicherheitsanforderungen erfolgt ebenfalls im Rahmen einer Schutzbedarfsanalyse. Dem Ergebnis folgend werden die Prozesse in Sicherheitsklassen eingeteilt.

8.3 Schutzbedarfsklassen

Die Transformation der Sicherheitsanforderungen auf entsprechende Sicherheitsmaßnahmen ist ein umfangreicher Vorgang. Wer daher statt frei definierbarer Sicherheitsanforderungen die im vorangegangenen Hauptkapitel erwähnten Schutzbedarfsklassen verwendet, kann jeweils spezifische Transformationen weitestgehend vermeiden und auf standardisierte Ergebnisse zurückgreifen. Dies steigert die Effizienz der Transformation und reduziert die Komplexität im Betrieb, schränkt andererseits aber – oftmals gewünscht – die Individualität ein.

Die unterste geforderte Schutzbedarfsklasse stellt das mindestens erforderliche Sicherheitsniveau dar, den Grundschutz. Hierbei kann

es durchaus sein, dass das Unternehmen später im Rahmen einer Überprüfung einen höheren als diesen anfangs ermittelten Grundschutz erreichen möchte. Dies hat dann Rückwirkung auf die Sicherheits-, Kontinuitäts- und Risikopolitik. Sie legt u. a. den Grundschutz fest, der für die gesamte ITK gültig ist.

8.4 Praxisbeispiele

Als Beispiel für die Praxis zeigt der folgende Ausschnitt die Detaillierung des Sicherheitskriteriums Verfügbarkeit für ein Informationssystem.

Bedrohungsklasse			Ausfall							...
Schutzobjekt			Rechner		Speicher		Standort		...	...
Anforderung	Wert	Charakteristikum	Rechnerverfügbarkeit	Rechnerredundanz	Plattenredundanz	Synchrone Spiegelung	Anzahl RZ-Standorte	RZ-Distanz	...	...
		Wichtigkeit								
Max. tolerierbare Ausfallzeit	1h	10	9	10	10	9	10	9	...	...
Max. tolerierbarer Datenverlust	1 min	9	9	9	9	10	9	9	...	...
...	...	...	...	...	...	...	...	...	...	...
Erfüllungsgrad insgesamt			...	...	...	...	...	...	...	...
Zielwert			99,99 %	100 %	100 %	100 %	2	10 km	...	...

Die Sicherheitstransformation kann auf die verschiedenen Sicherheitsklassen angewandt werden. Dadurch entstehen je Klasse standardisierte Sicherheitscharakteristika. Dies vereinfacht in der Folge die Umsetzung der fachlichen Sicherheitsanforderungen und die Abschätzung der entstehenden Aufwände.

Die folgende Tabelle zeigt auszugsweise ein prinzipielles Beispiel von Mindest-Sicherheitsmaßnahmen für ein Informationssystem, das unternehmensspezifisch überprüft und angepasst werden muss. Sicherheitsmaßnahmen umfassen Prozesse, Ressourcen und Organisa-

tion sowie Produkte und Dienstleistungen. Die Maßnahmen-Klassen-Matrix (MKM) bzw. Klassen-Maßnahmen-Matrix (KMM) des Autors wird nach ihrer Fertigstellung Teil der Sicherheitsarchitektur. Das spätere Unterkapitel der Sicherheitsarchitektur, auf das ein Element der Tabelle verweist, ist ein Ergebnis der Transformation.

Maßnahmen-Klassen-Matrix (MKM)	Verfügbarkeitsklasse			
Mindest-Sicherheitsmaßnahmen	V1	V2	V3	V4
Ersatzressourcen, z. B. Komponenten, Systeme, Räumlichkeiten, Personal, sind einsatz-/betriebsbereit innerhalb von ...	168 h	72 h	24 h	4 h
Vollständige Redundanz des IT-Systems	Nein	Nein	Ja	Ja
Gesicherte Infrastruktur je Standort (s. a. Kapitel Sicherheitsarchitektur, Ressourcen, Infrastruktur)	Nein	Ja	Ja	Ja
Zwei räumlich ausreichend voneinander entfernt gelegene Standorten	Nein	Ja	Ja	Ja
Tägliche Datensicherung und Auslagerung	Ja	Ja	Ja	Ja
Beschreibung des Datensicherungsverfahrens aktuell, getestet, geübt und für einen sachverständigen Dritten verständlich	Ja	Ja	Ja	Ja
Synchrone oder asynchrone Spiegelung der Daten auf das Back-up-System	Nein	Nein	Nein	Ja
Parallelbetrieb des Original- und Ausweichsystems	Nein	Nein	Nein	Ja
Wiederanlaufplan für den Übergang in den Notbetrieb sowie die Rückkehr in den regulären Betrieb vorhanden, aktuell und getestet	Nein	Ja	Ja	
Notbetriebsplan vorhanden, aktuell und getestet	Nein	Ja	Ja	Ja
Mitarbeiter zur Betriebskontinuität, z. B. Übergang in den Notbetrieb, Notbetrieb, Wiederherstellung, Rückkehr in den regulären Betrieb, geschult	Ja	Ja	Ja	Ja
Pfadanalyse hinsichtlich SpoFs durchgeführt	Nein	Nein	Nein	Ja
Betriebsunterbrechungsversicherung abgeschlossen	Nein	Nein	Nein	Ja
Anforderungsgerechte Verträge mit Dienstleistern/Herstellern abgeschlossen	Nein	Ja	Ja	Ja
...				
	Vertraulichkeitsklasse			
Mindest-Sicherheitsmaßnahmen	T1	T2	T3	T4
...				

8.5 Zusammenfassung

Zur Abbildung der Sicherheitsanforderungen auf entsprechende Sicherheitsmaßnahmen dient das vom Autor abgeleitete House of Safety, Security and Continuity (HoSSC). HoSSC fokussiert auf den Teilaspekt Sicherheit des House of Quality. Es stellt transparent dar, inwieweit die Sicherheitscharakteristika die Sicherheitsanforderungen erfüllen. Optional ermöglicht es die grafische Darstellung der Position von Wettbewerbern.

*House of Safety,
Security and
Continuity*

HoSSC bildet die Grundlage des Safety, Security and Continuity Function Deployment. In seinem Verlauf werden die Sicherheitsanforderungen erfasst, zu erreichende Zielwerte festgelegt und die Bedeutung der Anforderung gewichtet.

*Safety, Security
and Continuity
Function
Deployment*

Den Sicherheitsanforderungen werden Sicherheitscharakteristika gegenübergestellt. Beispielsweise kann die Anforderung nach max. 1 Stunde Ausfallzeit pro Jahr in den Zielwert 99,99 % des Sicherheitscharakteristikums Rechnerverfügbarkeit übersetzt werden. Für jedes Sicherheitscharakteristikum wird bewertet, in welchem Maß es die Sicherheitsanforderung erfüllt. Je Sicherheitscharakteristikum ergibt sich abschließend eine Summe. Sie gibt an, wie stark ein Sicherheitscharakteristikum alle gestellten Sicherheitsanforderungen abdeckt.

*Sicherheits-
charakteristika*

Hierauf aufbauend und unter Berücksichtigung auch nicht sicherheitsrelevanter Anforderungen erfolgt die Entscheidung, welches die kritischen und wichtigen Charakteristika sind.

Die Sicherheitscharakteristika werden weiter detailliert und konkretisiert. Aus der Verfügbarkeitsanforderung ergeben sich z. B. Anforderungen an ein fehlertolerantes Rechnersystem, Plattenspiegelung und zwei voneinander entfernt liegende Standorte.

Detaillierung

Aus den detaillierten Sicherheitscharakteristika ergeben sich Anforderungen an den Lebenszyklus des ITK-Systems. Sie müssen u. a. in der Kosten-Nutzen-Analyse, der technischen Spezifikation und dem Test sowie dem Betrieb berücksichtigt werden sowie in den Prozessen, wie z. B. dem Kapazitätsmanagement.

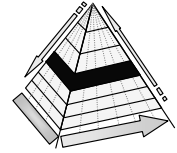
Lebenszyklus

Durch die Bildung von Schutzbedarfsklassen kann auf standardisierte Sicherheitslösungen zurückgegriffen werden.

*Schutzbedarfs-
klassen*

9 Sicherheitsarchitektur

Wie wir bisher gesehen haben, gibt die Sicherheits-, Kontinuitäts- und Risikopolitik den Rahmen für das Management dieser Themenfelder vor. Die zweite Ebene der Sicherheitspyramide spezifiziert die Sicherheitsziele bzw. Sicherheitsanforderungen. Die Sicherheitstransformation leitet hieraus Sicherheitscharakteristika für die jeweiligen Prozesse und Schutzobjekte sowie für jedes Sicherheitskriterium ab.



Die nächste Stufe der Sicherheitspyramide ist die Sicherheitsarchitektur. Sie stellt die Sicherheitscharakteristika in Form prinzipieller Sicherheitsmaßnahmen als eine Art „Baukasten“ von Sicherheitselementen zur Verfügung. Die Sicherheitsarchitektur bildet somit die Basis für die später beschriebenen Sicherheitsrichtlinien, -konzepte und -maßnahmen. Sie enthält ferner die aktuelle und zukünftige Architektur für alle PROSim-Elemente.

Die Sicherheitsarchitektur unterteilt sich ihrerseits in drei weitere Ebenen. Gemäß dem Sicherheitsdreiklang repräsentiert die erste Ebene die prinzipiellen und erhobenen Sicherheitsanforderungen und die zweite die prinzipiellen Bedrohungen. Die dritte Ebene unterteilt sich in allgemein nutzbare Sicherheitsprinzipien und -strategien sowie in Sicherheitselemente zur Absicherung des regulären Betriebs und zum Schutz vor Angriffen. Betrachten wir diese drei Zwischenebenen aus der Sicht des Risikodreiklangs statt aus der Sicherheitsperspektive, so korrespondieren sie mit dem Schadens-, Bedrohungs- und Schwachstellenpotenzial. Entsprechend der zweiten Dimension der Sicherheitspyramide enthält die Architekturebene die Prozess-, Ressourcen- und Organisationsarchitektur. Hieraus ergeben sich folgende Unterkapitel:

*Drei
Architektur-
ebenen*

1. Überblick
2. Prinzipielle Sicherheitsanforderungen
3. Prinzipielle Bedrohungen
4. Sicherheitsstrategien und -prinzipien
5. Sicherheitselemente
für Betriebs- und Angriffssicherheit sowie Kontinuität unter Berücksichtigung von Prozessen (Kern-, Support-, Begleitprozesse {Managementdisziplinen}), Ressourcen und Organisation (PROSim)
6. Hilfsmittel Sicherheitsarchitekturmatrix
7. Zusammenfassung

9.1 Überblick

*Der Weg zur
ITK-Sicher-
heitsarchitektur*

Wie gelangen Sie nun zu Ihrer unternehmensspezifischen Sicherheitsarchitektur? – Hierzu empfiehlt sich folgendes Vorgehen, das sich an den drei Dimensionen der Sicherheitspyramide orientiert: Aus der ersten Dimension, den hierarchischen Ebenen, haben wir – ausgehend von der Sicherheits-, Kontinuitäts- und Risikopolitik – die Sicherheitsziele bzw. -anforderungen erhoben. Um diese in Sicherheitselemente der Architektur zu überführen, können Sie in folgenden Schritten vorgehen:

1. Zusammenführung der Sicherheitsanforderungen, die sich aus den Schutzbedarfsanalysen ergeben haben, zu Sicherheitsklassen
2. Erhebung prinzipieller Bedrohungen und deren Eintrittswahrscheinlichkeit
3. Aufstellung von Strategien und Prinzipien zur Erhöhung des Sicherheits- und Kontinuitätsniveaus
4. Entwicklung von Sicherheitselementen zur Vermeidung, Verringerung und Verlagerung potenzieller Schwachstellen im Betrieb und gegenüber Angriffen, d. h. zur Risikoreduzierung bzw. zur Erhöhung des Sicherheits- und Kontinuitätsniveaus.

Nachdem die Sicherheitselemente entwickelt worden sind, werden sie entsprechend der zweiten Dimension im Hinblick auf folgende sicherheitsrelevanten Themenfelder betrachtet:

PROSim

- Prozesse bzw. Prozesselemente
- Ressourcen und
- Organisation.

Diese sind ausgerichtet auf das Sicherheitsmanagement, weshalb ich sie im Folgenden auch als PROSim bezeichne.

Die Sicherheitselemente innerhalb dieser Themenfelder können nach ihrer Charakteristik in folgende Kategorien weiter unterteilt werden:

- vorbeugend, pflegend, übend und überprüfend
- beobachtend, erkennend, meldend/alarmierend
- erwidern, abwehrend
- (schadens-)beurteilend, diagnostizierend
- wiederherstellend und
- verbessernd.

Die Sicherheitselemente und PROSim-Themenfelder können im Lebenszyklus eines Prozesses, einer Ressource (z. B. eines ITK-Systems), eines Produktes oder einer Dienstleistung Einfluss haben auf einzelne Prozessschritte bzw. Phasen oder auf den kompletten Ablauf bzw. alle Phasen. Dementsprechend gibt es phasenspezifische und phasenübergreifende Elemente.

Phasenspezifische und phasenübergreifende Elemente

Weiterhin sollten sowohl Elemente für die Betriebssicherheit (Safety) und Kontinuität (Continuity) vorgesehen werden als auch solche zur Sicherheit vor Angriffen (Security), um gegen die verschiedenartigen Bedrohungen gerüstet zu sein.

Betriebs- und Angriffs-sicherheit sowie Kontinuität

Die Sicherheitsarchitektur gibt somit einen Rahmen vor und verschafft einen Überblick über die möglichen, erforderlichen und vorhandenen Sicherheitselemente. Um diesen Überblick graphisch darzustellen, wird die Sicherheitspyramide entlang der PROSim-Elemente in einzelne pyramidenförmige Scheiben geschnitten. Für die so entstandenen Teilpyramiden kann für jede Hierarchieebene der Sicherheitspyramide, unterteilt nach vorbeugend, erkennend, abwehrend und prüfend, sowie für jede Phase des Lebenszyklus gekennzeichnet werden, welche Elemente erforderlich und welche vorhanden sind. Es ist leicht erkennbar, an welchen Stellen es „weiße Flecken“ gibt.

Überblick über Sicherheitselemente

Eine weitere Verfeinerung ergibt sich, wenn der Status der einzelnen Elemente jeder Teilpyramide in Ampelfarben und/oder mit einem Symbol dargestellt wird. Grün (☺) sind beispielsweise die vorhandenen und umgesetzten Elemente, gelb (☹) die in Entwicklung befindlichen und rot (⊗) diejenigen, die noch erstellt werden müssen.

Status in Ampelfarben und/oder mit Symbol

Entsprechend den Elementen des Sicherheitsdreiklangs beschäftigen sich die folgenden Kapitel mit

- prinzipiellen Sicherheitsanforderungen
- Prinzipiellen Bedrohungen
- Sicherheitsstrategien, -prinzipien und -elementen.

Sicherheitselemente beziehen sich auf die Prozesse, Ressourcen und die Organisation (PROSim), zu denen jeweils ein Überblick gegeben wird. Die Prozesse ihrerseits unterteilen sich in Kern-, Support- und Begleitprozesse. Wegen der Bedeutung der Begleitprozesse sind diese auf der gleichen Ebene wie der Überblick angesiedelt.

9.2 Prinzipielle Sicherheitsanforderungen

Im ersten Schritt auf dem Weg zur Sicherheitsarchitektur fassen wir die erhobenen Sicherheitsanforderungen zu prinzipiellen Sicherheitsanforderungen der eingesetzten ITK-Systeme zusammen und konsolidieren sie. Die Sicherheitsanforderungen berücksichtigen u. a. gesetzliche, kunden- und unternehmensspezifische Vorgaben.

*Primäre
Sicherheits-
kriterien*

Zur Ermittlung der prinzipiellen Anforderungen ordnen wir die individuellen Sicherheitsanforderungen der Informationssysteme den primären Sicherheitskriterien Konformität, Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität zu. Je Sicherheitskriterium lassen sich Klassen bilden, die bei zukünftigen Schutzbedarfsanalysen genutzt werden.

*Sekundäre
Sicherheits-
kriterien*

In gleicher Weise führen wir die Anforderungen hinsichtlich der sekundären Sicherheitskriterien, z. B. Nachvollziehbarkeit, Nachweisbarkeit, Alarmierungs-, Erkennungs- und Abwehrfähigkeit zusammen.

Ein Überblick in Form der Anforderungsarchitektur (requirements architecture) fasst die so erhobenen Sicherheitsanforderungen zusammen.

9.3 Prinzipielle Bedrohungen

*Konzentration
auf prinzipielle
Bedrohungen*

Es gibt eine Vielzahl möglicher Auslöser und Bedrohungen, z. B. durch Feuer, Flüssigkeit, und technischen Defekt. Durch Abstraktion einerseits und Konzentration auf die Auswirkungen andererseits können diese eingeschränkt und überschaubar gestaltet werden. Zur Früherkennung, Vermeidung oder Wiederherstellung müssen sie zwar individuell betrachtet werden, sollten jedoch durch Abstraktion zu Bedrohungsgruppen zusammengefasst werden, gegen die gleiche oder weitestgehend gleiche Maßnahmen ergriffen werden können. Die auf unterschiedlichen Auslösern und/oder Bedrohungen basierenden Auswirkungen bezeichnet der Autor als prinzipielle Bedrohungen. Sie sind in der folgenden Aufzählung beispielhaft dargestellt:

- Ausfall oder Einschränkung von Ressourcen
 - (externe) Versorgungseinrichtungen, z. B. Strom, Gas, Wasser, Kommunikation (Ursache z. B. Beschädigung bei Bauarbeiten, technische Defekte, Flugzeugabsturz, Sturm, Sabotage, Terrorismus, Verseuchung)

- externe Dienstleister, z. B. Lieferanten, Software-Häuser, Service-Geber (Outsourcing, Managed Services) (Ursache z. B. Insolvenz, Ausfall der ITK-Infrastruktur oder Haustechnik, Streik, Service-Defizite, Terrorismus)
- Gebäude oder Räumlichkeiten (Ursache z. B. Brand, Rohrbruch, geplatzter Sprinklerkopf, Kühlflüssigkeit der Klimaanlage, Überflutung {Fluss, See, Schneeschmelze, Grundwasser}, Flugzeugabsturz, Sturm, Erdbeben, Terrorismus)
- Gebäude-, Raum-Infrastruktur und Haustechnik (z. B. Strom oder Klima) (Ursache z. B. Brand, Explosion, Rohrbruch, geplatzter Sprinklerkopf, Kühlflüssigkeit der Klimaanlage, Abwasser, Überflutung {Fluss, See, Schneeschmelze, Grundwasser}, Überspannung, Beschädigung, Wartungsfehler)
- ITK-Infrastruktur (Ursache, z. B. Brand, Explosion, Feuchtigkeit, Fehlbedienung, Software-Fehler, technischer Defekt, Stromausfall, Überspannung, Staub, Rauch, Vibrationen, Beschädigung, Wartungsfehler, Überlastung)
- Personal (Ursache z. B. Lebensmittelvergiftung, Krankheit, Unfall, Tod, blockierte Anfahrt zur Arbeit {gesperrte Autobahnen, wegen Oberleitungsschaden oder Stellwerksausfall stehende Bahnen})
- Blockade
 - Kommunikationsanbindung (Ursache z. B. Denial-of-Service-Attacken)
 - Gebäudezutritt (Ursache z. B. Streik, Demonstration, Ausfall des Zutrittskontrollsystems)
- Beschädigung oder Verlust, z. B. von Einrichtungsgegenständen, Computer-Equipment, Akten, Verträgen, Dokumenten, Dateien, Datenbeständen (Ursache z. B. Einbruch, Vandalismus, Diebstahl, Brand, Wasser)
- Verfälschung, z. B. von Daten (Ursache z. B. Fehleingabe aufgrund von Tippfehlern oder Medienbrüchen, Software-Fehler, fehlende Plausibilisierung von Daten, inkonsistente redundante Datenhaltung, direkte Manipulation, Viren)
- Täuschung durch Vorspiegelung einer falschen Identität (z. B. Vortäuschung einer falschen Benutzeridentität, Vortäuschung einer falschen IP-Absenderadresse {IP-Spoofing})
- unzulässige Informationsgewinnung, z. B. über Betriebsgeheimnisse, geheime Forschungsergebnisse, Kundendaten, Lieferkonditionen (Ursache z. B. Abhören von drahtgebundener oder drahtloser Übertragung oder von Räumen, Ausspähen, Spionage)

{z. B. durch Vertrauenserschleichung und social engineering}, aber auch Phishing, Spyware und Adware sowie unzulässiger Zugriff auf vertrauliche Daten)

- unzulässige Nutzung der Unternehmensinfrastruktur, z. B. von ITK-Systemen, Telefonen (für teure Auslandstelefonate) oder Kopieren.

Als Beispiel für Bedrohungen kann die unzulässige Informationsgewinnung bei unverschlüsselt übertragenen Texten dienen. Der Angreifer hört die unverschlüsselten Datenpakete ab.

Einen Überblick über die prinzipiellen Bedrohungen, ihre Ursachen und die jeweils betroffenen Objekte erhalten Sie durch eine Matrixdarstellung. Den Objekten werden die prinzipiellen Bedrohungen bzw. Szenarien gegenübergestellt und in den Schnittpunkten der Matrix die dazugehörigen Auslöser eingetragen. Es entsteht eine Bedrohungslandkarte.

Bedrohungslandkarte					
Bedrohungs- kategorie		Ausfall, Einschränkung	Blockade	Beschädigung, Verlust	...
Objekt und Klasse					
Externe Versorgungseinrichtungen, z. B.		Beschädigung, Sabotage, Terrorismus, ...	...	...	...
- Strom					
- Gas					
- Wasser					
- Kommunikation					
Externe Dienstleister, Lieferanten, Service-Geber		Insolvenz, ...	...	...	...
Gebäude		...	...	...	...
Räumlichkeiten		...	...	...	...
Gebäude-Infrastruktur		...	...	...	...
IT-Infrastruktur		...	...	...	...
Personal		...	...	...	...
...		...	...	...	...

*Bedrohungs-
potenzial*

In dieser oder einer separaten Matrix können Sie eintragen, wie hoch Sie die Eintrittswahrscheinlichkeit des jeweiligen Ereignisses einschätzen. Sie erhalten dadurch das Bedrohungspotenzial der jeweiligen Bedrohung. Das entsprechende Feld der Matrix kann dann gemäß der Eintrittswahrscheinlichkeit farblich hinterlegt werden. Bei

einer dreistufigen Einteilung können Sie beispielsweise die Ampelfarben rot, gelb, grün verwenden.

Da Absicherungen üblicherweise nicht gegen alle denkbaren Bedrohungen erfolgen, ist die Eintrittswahrscheinlichkeit ein Indiz dafür, mit welcher Priorität Schutzmaßnahmen unter Kosten-Nutzen-Erwägungen ergriffen werden sollten. Wie bereits an anderer Stelle ausgeführt, ist zu beachten, dass eine Bedrohung trotz einer sehr geringen Eintrittswahrscheinlichkeit dennoch sehr kurzfristig auftreten kann, d. h. morgen, in den nächsten Stunden oder auch im nächsten Augenblick. Ebenfalls zu berücksichtigen ist, dass Eintrittswahrscheinlichkeiten oftmals retrospektiv sind. D. h. sie basieren auf der Häufigkeit eines Ereignisses in der Vergangenheit. Dementsprechend können derartige Eintrittswahrscheinlichkeiten mehr oder weniger häufigen Veränderungen unterliegen.

Es empfiehlt sich, eine unternehmensweit geltende standardisierte prinzipielle Bedrohungsmatrix zu erstellen. Sie gibt zum einen an, welche Bedrohungen berücksichtigt werden sollen. Zum anderen enthält sie die jeweilige Einschätzung der Eintrittswahrscheinlichkeit, sofern diese innerhalb des Unternehmens allgemeingültig ist. Gilt eine Bedrohung als „gesetzt“, d. h. soll sie unabhängig von der Eintrittswahrscheinlichkeit berücksichtigt werden, so wird die Eintrittswahrscheinlichkeit auf 1 gesetzt. Bei prinzipiellen Bedrohungen, die individuell eingeschätzt werden müssen, wird das entsprechende Feld der Matrix leer gelassen.

*Standardisierte
prinzipielle
Bedrohungsmatrix*

Diese zentrale Bedrohungsmatrix, der Autor bezeichnet sie als Bedrohungsarchitektur, erspart den Prozess- und Ressourcenverantwortlichen eines Unternehmens in vielen Fällen die individuelle Einschätzung der verschiedenen Bedrohung und wirkt damit effizienzfördernd. Gleichzeitig erhöht dies die Konsistenz der Eintrittswahrscheinlichkeiten sowie die Durchgängigkeit und zielgerichtete Vollständigkeit der Bedrohungen. Es verbleiben dann jene für den jeweiligen Geschäftsprozess oder die jeweilige Ressource spezifischen Bedrohungen und die Prüfung der Bedrohungsmatrix auf Angemessenheit hinsichtlich der individuellen Gegebenheiten. So kann der Ausfall eines Rechnersystems oder Gebäudes als „gesetzt“ gelten, während die Bedrohung durch Hochwasser bei mehreren Standorten eines Unternehmens lokationsabhängig zu bewerten ist.

Effizienzgewinn

9.4 Strategien und Prinzipien

Für den zielgerichteten und wirtschaftlichen Aufbau des Sicherheitsmanagements ist es wesentlich, das Spektrum der einsetzbaren

Strategien im Hinblick auf Sicherheit und Risiko sowie der Sicherheitsprinzipien zu kennen. Hierdurch können einseitige Entscheidungen im Interesse einer ausgewogenen, gesamtheitlichen und wirtschaftlichen Lösung vermieden werden. Die folgenden Unterkapitel geben einen Überblick zu folgenden Prinzipien und Strategien:

1. Risikostrategie
2. Sicherheitsstrategie
3. Prinzip der Wirtschaftlichkeit
4. Prinzip der Abstraktion
5. Prinzip der Klassenbildung
6. Poka-Yoke-Prinzip
7. Prinzip der Namenskonventionen
8. Prinzip der Redundanz
9. Prinzip des „aufgeräumten“ Arbeitsplatzes
10. Prinzip des „gesperrten“ Bildschirms
11. Prinzip der Eigenverantwortlichkeit
12. Vier-Augen-Prinzip
13. Prinzip der Funktionstrennung
14. Prinzip der Sicherheitsschalen
15. Prinzip der Pfadanalyse
16. Prinzip des generellen Verbots
17. Prinzip der minimalen Rechte
18. Prinzip der minimalen Dienste
19. Prinzip der minimalen Nutzung
20. Prinzip der Nachvollziehbarkeit und Nachweisbarkeit
21. Prinzip des „sachverständigen Dritten“
22. Prinzip des Closed-Shop-Betriebs und der Sicherheitszonen
23. Prinzip der Prozess-, Ressourcen- und Lebenszyklusimmanenz
24. Prinzip der Konsolidierung
25. Prinzip der Standardisierung
26. Prinzip der Plausibilisierung
27. Prinzip der Konsistenz
28. Prinzip der Untergliederung
29. Prinzip der Vielfältigkeit

9.4.1 Risikostrategie (Risk Strategy)

Um die Sicherheit, genauer das Sicherheits- und Kontinuitätsniveau zu erhöhen, bzw. die Risikolage zu verbessern, gibt es für die verschiedenen Risiken folgende Strategien in Form der Müllerschen 4Vs bzw. des Müllerschen V-Quadrupels des Risikomanagements:

- Vermeidung
- Verringerung (z. B. Verteilung)
- Verlagerung (z. B. durch Versicherung, geeignete Vertragsgestaltung mit Kunden und Lieferanten oder Outsourcing)
- Vereinnahmung, d. h. Übernahme, verbleibender Risiken.

Für jedes Risiko muss abgewogen werden, welche Strategie oder Strategiekombination unter Kosten-Nutzen-Aspekten verfolgt werden soll. Hierbei kann die Schadenklassifizierung gemäß der Abbildung Orientierung geben.

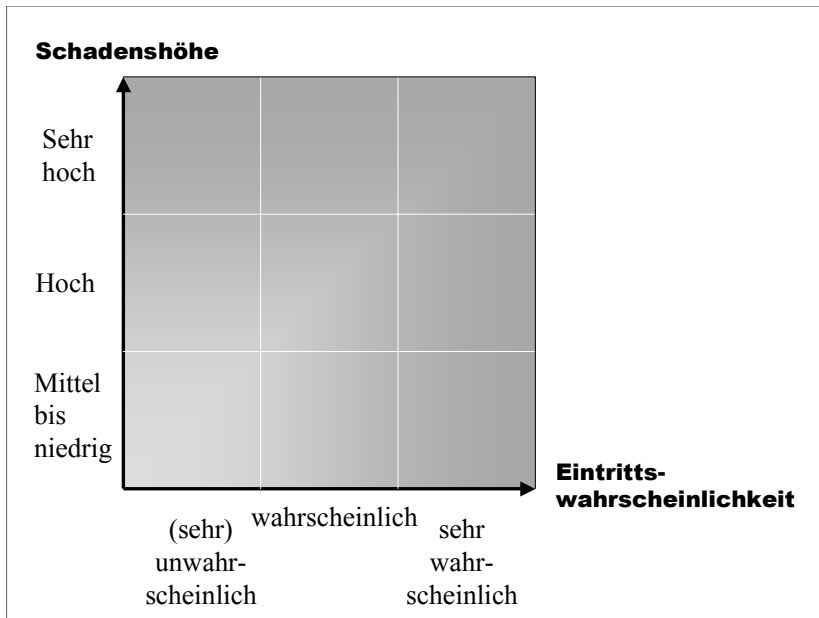


Abb. 9.1: Schadenklassifizierung

Die dortigen Begriffe „sehr hoch“ bis „niedrig“ und „(sehr) unwahrscheinlich“ bis „sehr wahrscheinlich“ bedürfen der unternehmensspezifischen Quantifizierung. So kann bei einem spezifischen Unternehmen „sehr hoch“ mit einem Schadenswert von > 1 Mio. EUR

quantifiziert sein und „(sehr) unwahrscheinlich“ mit einer Eintrittswahrscheinlichkeit von seltener als alle 1.000 Jahre.

9.4.2 Sicherheitsstrategie (Safety, Security and Continuity Strategy)

Die Sicherheitsstrategie legt fest, welche Maßnahmenfolge zur Vermeidung oder Verringerung eines Risikos ergriffen werden sollte. Die einzelnen Elemente der Sicherheitsstrategie bestehen aus Maßnahmen zur

- Vorbeugung (Prävention), Pflege, Übung und Überprüfung (Verifikation)
- Beobachtung (Monitoring), Erkennung (Detektion), Meldung/Alarmierung
- Erwidern (Reaktion), z. B. Abwehr
- Beurteilung (Evaluation) des Schadens
- Wiederherstellung (Restauration)
- Verbesserung (Emendation).

Beispiel
Netzanbindung

Ein konkretes Beispiel für die Anwendung der Sicherheitsstrategie zum Schutz vor Angriffen ist die Anbindung des Unternehmensnetzes an das Internet. Als Präventivmaßnahme wird eine Firewall installiert, die das zu schützende Netz vor Übergriffen aus dem unsicheren Netz schützt. Gleichzeitig hat die Firewall die Aufgabe, sicherheitsrelevante Zugangsversuche bzw. Ereignisse zu erkennen, abzuwehren und zu melden. Das Intrusion-Detection-System dient der Erkennung von Angriffen und der Alarmierung, das Intrusion-Response-System leitet die zeitnahe Reaktion ein, indem beispielsweise die Firewall umkonfiguriert wird.

Im Falle eines Angriffs wird darüber hinaus versucht, den Eigentümer der IP-Adresse ausfindig zu machen und die Angriffsroute zurück zu verfolgen.

Es erfolgt eine Beurteilung des Schadensausmaßes und der aktuellen Situation. Dementsprechend werden Maßnahmen eingeleitet. Zum frühest möglichen Zeitpunkt beginnt die Wiederherstellung für den regulären Betrieb. Der Vorfall wird ausgewertet, um eventuelle neue Erkenntnisse zu sammeln und für Verbesserungen zu nutzen.

Die ergriffenen Maßnahmen werden kontinuierlich gepflegt und ihre Wirksamkeit in regelmäßigen Abständen überprüft.

9.4.3 Prinzip der Wirtschaftlichkeit

Sicherheit soll dem Unternehmenszweck und den Unternehmenszielen dienen. Daher sind alle sicherheitsrelevanten Aktivitäten auf Wirtschaftlichkeit hin auszurichten, d. h. unter Kosten-Nutzen-Aspekten zu betrachten. Dies erfordert einerseits die Kenntnis der Anforderungen, der Bedrohungen und der Auswirkungen sowie andererseits des Aufwands für die Realisierung und den Betrieb der entsprechenden Lösung.

9.4.4 Prinzip der Abstraktion

An unterschiedlichen Standorten eines Unternehmens und bei den verschiedenen Betriebssystemen werden von den Verantwortlichen nach bestem Wissen und Gewissen Sicherheitsmaßnahmen ergriffen. Fehlende Vorgaben führen jedoch zu unterschiedlichen Sicherheitsniveaus. Die Vernetzung der Systeme kann dann dazu führen, dass alle Systeme auf das niedrigste Sicherheitsniveau heruntergezogen werden.

Problem:
Unterschied-
liches Sicher-
heitsniveau

Dem kann entgegengewirkt werden, indem im Vorfeld plattform-/betriebssystemunabhängige bzw. -übergreifende Vorgaben gemacht werden. Alternativ können bereits existierende Sicherheitsmaßnahmen abstrahiert werden, sodass sie zukünftig betriebssystemübergreifend wirken. Hierdurch erreichen Sie zum einen eine Standardisierung und zum anderen eine Know-how-Sicherung. Die abstrahierten Vorgaben werden in Form von Sicherheitsrichtlinien dokumentiert. Bei jeder neuen Plattform bilden sie die Grundlage für die spezifische Konfiguration. Dies ist ein wirtschaftliches Mittel, um bei neuen technologischen Entwicklungen auf bereits erprobtem Wissen aufsetzen zu können.

Lösung:
abstrahierte
plattform-
übergreifende
Vorgaben

Das Prinzip der Abstraktion lässt sich auch auf das Management von Systemen übertragen. Sei es die Benutzerverwaltung, die von Betriebssystem zu Betriebssystem unterschiedlich ist, die Verwaltung von Netzen oder Speichernetzwerken. Sie alle fordern spezifische Kenntnisse im Management jedes einzelnen Systems. Solange die IT-Landschaft klein oder der IT-Bereich in der Lage ist, eine unternehmensweit einheitliche Plattformstrategie durchzusetzen, ist Abstraktion weniger wichtig. Bei großen heterogenen Installationen jedoch steigen die Komplexität und das erforderliche Wissensspektrum enorm an. Abstrahierende Managementsysteme, wie z. B. ein plattformübergreifendes Benutzerverwaltungssystem, vereinfachen diese Aufgaben durch Vereinheitlichung, reduzieren die Komplexität und helfen dadurch, Bedienungsfehler zu vermeiden.

Plattform-
übergreifende
Management-
systeme

9.4.5 Prinzip der Klassenbildung

Maßgeschneiderte gegenüber standardisierter Lösung

Die Sicherheitsanforderungen der Geschäftsprozesse und daraus abgeleitet die der Informationssysteme sind üblicherweise unterschiedlich. Es ergibt sich somit eine Vielzahl mehr oder weniger unterschiedlicher Sicherheitsmaßnahmen. Diese Lösungen müssen jeweils individuell entwickelt und anschließend verwaltet und gepflegt werden. Der im Einzelfall optimalen maßgeschneiderten Lösung stehen die Vielzahl, die daraus resultierende Komplexität sowie die informationssystemübergreifende Wirtschaftlichkeit gegenüber.

Klassenbildung

Es empfiehlt sich daher, unternehmensspezifisch geeignete Sicherheitsklassen zu bilden, um die Menge individueller Lösungen auf eine überschaubare, standardisierte und wirtschaftliche Anzahl von Lösungen zu reduzieren.

Verfügbarkeitsklassen

Beispielsweise gibt es hinsichtlich der Verfügbarkeit von ITK-Systemen in der Regel unterschiedliche Anforderungen. Diese gilt es in geeigneten Verfügbarkeitsklassen zusammenzuführen, um ihre Anzahl zu reduzieren sowie überschaubar und effizient zu machen. Die Verfügbarkeitsklassen richten sich nach der maximal zulässigen Ausfalldauer eines ITK-Systems. Sie können beispielsweise folgendermaßen definiert sein:

- max. Ausfalldauer: 0 h, d. h. unterbrechungsfreier Rund-um-die-Uhr-Betrieb
- max. Ausfalldauer: 4 h
- max. Ausfalldauer: 24 h
- max. Ausfalldauer: 5 Arbeitstage.

Da sich die Verfügbarkeitsklassen aus den Sicherheitsanforderungen ergeben haben, müssen in der Architektur Sicherheitselemente vorhanden sein, durch welche die Anforderungen der jeweiligen Klasse realisiert werden können. Aus diesen werden später Sicherheitsrichtlinien, -konzepte und -maßnahmen entwickelt.

Vertraulichkeitsstufen

Ähnliches gilt für die anderen Sicherheitskriterien, z. B. auch für das Sicherheitskriterium Vertraulichkeit. Anforderungsabhängig können verschiedene Vertraulichkeitsstufen gebildet werden, beispielsweise „öffentlich“, „unternehmensintern“, „vertraulich“, „geheim“.

9.4.6 Poka-Yoke-Prinzip

Die Vermeidung (Yoke) unbeabsichtigter Fehler (Poka) durch menschliches Handeln ist beim Thema Sicherheit ein wichtiger Gesichtspunkt.

Das Prinzip des „narrensicheren“ Mechanismus (Poka-Yoke) [23] dient dazu, Fehler von vornherein zu vermeiden, oder zur Fehlervermeidung die Aufmerksamkeit von Personen zu erlangen, z. B. durch akustische oder visuelle Signale. Müssen beispielsweise Bauteile zusammengesetzt werden, so lassen sich Fehler präventiv vermeiden, wenn die Verbindungen so gestaltet sind, dass sie nur auf eine einzige Art zusammenpassen und zusammengehörende Verbindungen die gleiche Farbe besitzen.

*„narren-
sicherer“
Mechanismus*

Gegenbeispiel: Notaus-Schalter



Das Rechenzentrum eines Unternehmens ist in einem nachträglich umgerüsteten Raum untergebracht. Hierzu wurde auf dem vorhandenen Boden ein Doppelboden aufgebaut, auf dem sich die Computeranlagen befinden. Nach dem Eintritt in das Rechenzentrum führt gleich rechts eine Rampe auf diesen Doppelboden. An der Wand neben der Rampe befindet sich in Schulterhöhe der offen liegende und unbeschriftete Notaus-Schalter, der im Vorbeigehen mit der Schulter ausgelöst werden kann.

Gegenbeispiel: Datenschutz



Die Darmstädter Polizei veröffentlichte laut Darmstädter Echo vom 16. Januar 2007 aufgrund eines „einmaligen, bedauerlichen“ Versehens 41 Einsatzberichte aus dem Zeitraum vom 6. bis zum 12. Februar 2006 im Internet. Dem Zeitungsbericht zufolge listeten diese neben Namen, Geburtsdatum und Adresse auch Automarke, Kennzeichen und Gesetzesverstoß sowie eventuelle Vorstrafen auf. Eine Bestätigungsabfrage, ob die Dateien wirklich ins Internet gestellt werden sollen, existierte dem Bericht zufolge jedoch nicht.

Im Hinblick auf den Zutritt zu Technikräumen oder zum Rechenzentrum oder den Zugang zu Informationssystemen und den Zugriff auf Daten bedeutet dies, dass nur die Personen eine entsprechende Berechtigung erhalten, die diese Berechtigung benötigen und entsprechend qualifiziert sind. Letzteres setzt gegebenenfalls eine entsprechende Schulung oder Weiterbildung voraus.

*Beispiel
Zutritt,
Zugang und
Zugriff*

Bei Informationssystemen bedeutet das Poka-Yoke-Prinzip, dass die Benutzeroberfläche leicht verständlich und einheitlich gestaltet sein muss, sodass sie intuitiv bedienbar ist. Einheitlichkeit äußert sich z. B. in der Anordnung gleicher Oberflächenelemente, in der Farbgebung und in der Einheitlichkeit der verwendeten Nomenklatur, die gleichzeitig auf die Kenntnisse und den Sprachgebrauch des Anwenders zugeschnitten sein sollte.

*Benutzer-
oberfläche*

Darüber hinaus sollten dem Benutzer nur die Funktionen angeboten werden, für die er berechtigt ist und die in dem aktuellen Kontext

*Plausibilitäts-
prüfung*

auch ausführbar sind. Die Vermeidung unzulässiger Eingaben und frühzeitige Plausibilitätsprüfungen dienen ebenfalls dazu, ein Informationssystem „narrensicher“ zu gestalten. Bei potenziellen Fehlbienungen oder risikoreichen Funktionen erhält der Benutzer eine Warnung (z. B. beim Löschen von Datensätzen oder Dateien).

*Fehler-
meldungen*

Fehlermeldungen sollten – anstatt Fehlercodes auszugeben – selbst-erklärend und auf die Kenntnisse des Anwenders zugeschnitten sein. Bei Fehlern sollten Hinweise auf das weitere Vorgehen gegeben werden. Onlinehilfe und kontextsensitive Hilfe sind erforderlich.

9.4.7 Prinzip der Namenskonventionen

Häufig vergeben Unternehmen Bezeichnungen zur Identifikation von Objekten. Ein Beispiel hierfür ist die Inventarisierung von Mobiliar, Hardware etc. Bezeichnungen gibt es darüber hinaus zur uneindeutigen, d. h. umkehrbar eindeutigen, Identifikation von Servern, Netzkomponenten, Programmen, Projekten, Mitarbeitern, Benutzerkennungen, Dokumenten etc. Um die Uneindeutigkeit und Nachvollziehbarkeit zu erreichen, empfiehlt es sich, einheitliche Schemata, die jeweiligen Namenskonventionen, zu definieren.

9.4.8 Prinzip der Redundanz (Principle of Redundancy)

Den Bedrohungen durch Ausfall lässt sich häufig durch Redundanz begegnen, indem „Single Points of Failure“ vermieden werden. Redundanz lässt sich durch folgende Kriterien charakterisieren:

1. Redundanzkategorien
2. Strukturelle Redundanz
3. Redundanzgrad (Redundanzquantität)
4. Redundanzgeschwindigkeit
5. Redundanzqualität

*Redundanz-
kategorien*

Überlegungen zur Redundanz beziehen sich auf eine Vielzahl von Objekten, z. B. eine Telefonanlage, einen speziellen Computer und Anwendungssoftware. Diese Objekte fasse ich nach ihrem Typus in Redundanzkategorien zusammen. Redundanzkategorien repräsentieren die Prozesse sowie alle Ressourcen, die von Prozessen genutzt werden, d. h. die Schutzobjekte.

*Strukturelle
Redundanz*

Redundanz wird häufig im Hinblick auf strukturelle Redundanz betrachtet. Diese erreichen Sie durch Hinzufügen weiterer gleichartiger Objekte, z. B. durch Duplizierung eines Gebäudes, einer Anlage oder eines Rechners. So verringert eine zweite räumlich hinreichend getrennte Netzanbindung die lokale Bedrohung durch Beschädigung

eines Stromversorgungskabels bei Bauarbeiten. Dasselbe gilt für andere Versorgungseinrichtungen, wie z. B. Wasser, Gas und Kommunikation. Dies kann auf weitere Objekte ausgedehnt werden, indem beispielsweise das Rechenzentrum dupliziert und an zwei Standorten betrieben wird, redundante räumlich ausreichend getrennte Arbeitsplätze zur Verfügung stehen, Hardware dupliziert wird, Stellvertreter vorhanden und Ersatzprozesse festgelegt sind. Bei speziellen fehlertoleranten Rechnern führt das Redundanzprinzip dazu, dass Komponenten sich selbst prüfen und bei Fehlern automatisch auf die alternative funktionsfähige Komponente umschalten. Wird Redundanz durch das Hinzufügen weiterer Komponenten, z. B. durch Duplizierung, erreicht, handelt es sich um eine strukturelle Redundanz.

Um eine vollständige strukturelle Redundanz zu erreichen, müssen alle beteiligten Elemente redundant gestaltet sein, sodass kein „Single Point of Failure“ mehr vorhanden ist.

*Vollständige
strukturelle
Redundanz*

Beispiel Stromversorgung

Eine geforderte und unter Kosten-Nutzen-Aspekten vertretbare Redundanz der Stromversorgung kann folgendermaßen hergestellt werden: Es wird eine unterbrechungsfreie Stromversorgung (USV) und eine Netzersatzanlage (NEA) installiert, alle Kabel werden redundant und in räumlich hinreichend getrennten Brandabschnitten verlegt, Komponenten, wie z. B. Trafos, werden redundant gestaltet, usw.



Je nach Umfang der Redundanz unterscheide ich verschiedene Redundanzgrade. Besitzt ein Objekt eine 100 %ige Redundanz, so ist es um 100 % überdimensioniert und daher im regulären Betrieb nur zur Hälfte ausgelastet bzw. belastet. Bei gleichzeitig vorliegender struktureller Redundanz bedeutet 100 %ige Redundanz, dass das Objekt gegen einen einfachen Ausfall geschützt ist, bei 200 %iger Redundanz ist es gegen zwei Ausfälle geschützt. Da in diesen Fällen 100 % bzw. 200 % der Kapazität im regulären Betrieb zuviel vorhanden sind, ist diese Vorgehensweise wirtschaftlich meist nicht vertretbar.

*Redundanz-
grade,
Redundanz-
quantität*

Rechenzentren können aus Wirtschaftlichkeitsgründen beispielsweise auf 50 %ige Redundanz ausgelegt sein. Bei gleichzeitiger struktureller Redundanz ersetzen sich hierbei zwei räumlich getrennte und im regulären Betrieb parallel betriebene Rechenzentren im Katastrophenfall gegenseitig, wobei jedes im regulären Betrieb auf 75 % der benötigten Leistung bzw. Kapazität dimensioniert ist. Bei Ausfall eines Rechenzentrums muss das andere somit dessen Aufgaben mit übernehmen.

Double-Source-Konzept

Selbst bei einem Redundanzgrad von 0 % lässt sich das Ausfallrisiko eines Standortes, eines Gebäudes, unternehmenskritischer ITK-Systeme und Services reduzieren, indem das Double-Source-Konzept, also strukturelle Redundanz, genutzt wird. Statt das Gesamtunternehmen oder das Rechenzentrum beispielsweise an einem Standort zu konzentrieren, befinden sich jeweils 50 % an zwei Standorten. Bei Ausfall der einen Hälfte sind somit weiterhin 50 % verfügbar. Auch derartige Lösungen erfordern üblicherweise Zusatzinvestitionen und beeinflussen die unternehmensinterne Kommunikation.

N+1-Redundanz

In Fachkreisen üblich ist der Begriff N+1-Redundanz bzw. das N+1-Prinzip. Hierbei werden im Betrieb N von N+1 gleichartigen Komponenten parallel betrieben, z. B. USVs, Transformatoren, Klimaanlage. Fällt eine dieser Komponenten aus, so steht eine weitere bereit, um deren Aufgabe zu übernehmen. Somit stehen insgesamt N+1 Komponenten zur Verfügung, obwohl ohne Redundanz nur N benötigt würden.

Redundanzlatenz, Redundanzgeschwindigkeit

Ein weiteres Charakteristikum für die Redundanz ist die Latenzzeit, d. h. die Redundanzlatenz, die vergeht, bis das redundante Objekt zum Einsatz kommt. Diese Angabe ist dann ausreichend, wenn das Objekt nur als Ganzes zum Einsatz kommt. Kommt das Objekt oder eine Gruppe gleichartiger Objekte erst nach und nach zum Einsatz, so wird die bereitgestellte Zielredundanz erst im zeitlichen Verlauf erreicht. Es ergibt sich somit eine Zunahme aktivierter redundanter Objekte pro Zeiteinheit, die Redundanzgeschwindigkeit.

Dementsprechend lassen sich folgende Redundanzlatenzen bzw. Redundanzgeschwindigkeiten unterscheiden: bei aktiver oder „heißer“ Redundanz läuft der Betrieb bei Ausfall einer Komponente quasi unbemerkt und unterbrechungsfrei weiter, die Latenzzeit ist annähernd 0, die Redundanzgeschwindigkeit nahe unendlich. Bei semiaktiver oder „warmer“ Redundanz ist ein überschaubarer Zeitraum erforderlich, um auf das redundante Objekt überzugehen. In diesem Fall ist das redundante Objekt üblicherweise in Betrieb, es sind jedoch beispielsweise laufende Anwendungen zu stoppen und gegebenenfalls Daten zu sichern sowie andere Daten einzuspielen und Anwendungen zu starten. Passive oder „kalte“ Redundanz bedeutet, dass eine Ersatzlösung vorhanden ist, bis zu ihrer Inbetriebnahme aber einige Zeit vergeht. Im Falle eines Ersatzservers muss der Systembetreuer beispielsweise diesen oder die erforderlichen Komponenten erst aus dem Lager holen, Hardware zusammenbauen und konfigurieren, Software installieren und konfigurieren sowie Daten einspielen, etc. Sind mehrere Server betroffen, so geht im Zeitverlauf einer nach dem anderen in Betrieb. Ähnliches gilt, wenn das Unter-

nehmen an einem anderen Standort sukzessive Ersatzarbeitsplätze aufbaut.

Bei sehr hohen Verfügbarkeitsanforderungen gerät ein weiteres Kriterium der Redundanz ins Visier, die Qualität der Redundanz. Was ist hierunter zu verstehen? Zur Erreichung einer Redundanz werden Komponenten häufig dupliziert. Besitzen diese Hardware- oder Software-Komponenten jedoch einen prinzipiellen Fehler, der in einer bestimmten Situation auftritt und einen Ausfall verursacht, so werden wohl auch die anderen Komponenten in dieser Situation ausfallen. Eine qualitativ höherwertige Lösung lässt sich z. B. durch den Einsatz gleichwertiger Komponenten unterschiedlicher Hersteller erreichen. Bei extrem hohen Sicherheitsanforderungen kann dies dazu führen, dass verschiedene Teams dieselbe Software für unterschiedliche Computer mit unterschiedlichen Betriebssystemen, Datenbanken etc. entwickeln. Dem prinzipiellen qualitativen Sicherheitsgewinn durch den Einsatz funktional gleicher Systeme verschiedener Hersteller oder Entwicklungsteams steht der Nachteil prinzipiell höherer Kosten in der Entwicklung und im Betrieb gegenüber.

*Redundanz-
qualität*

9.4.9 Prinzip des „aufgeräumten“ Arbeitsplatzes (Clear Desk Policy)

Dieses Prinzip besagt, dass jeder Mitarbeiter verpflichtet ist, seinen Arbeitsplatz „aufgeräumt“ zu hinterlassen. Dies beinhaltet auch, dass der Zugang zu Datenträgern und Unterlagen für Unbefugte gesperrt ist.

9.4.10 Prinzip des „gesperrten“ Bildschirms (Clear Screen Policy)

Dieses Prinzip besagt, dass jeder Mitarbeiter verpflichtet ist, seinen Bildschirm bei Abwesenheit vom Arbeitsplatz zu sperren, so dass der Einblick in Daten sowie der Zugang zu Informationssystemen und Daten für unberechtigte Dritte gesperrt ist.

9.4.11 Prinzip der Eigenverantwortlichkeit

Jeder Mitarbeiter ist für die von ihm durchgeführten Aktivitäten selbst verantwortlich. Dies bezieht sich u. a. auch auf Aktivitäten, die mit seinem Wissen oder grob fahrlässig veranlasst unter seiner Identität durchgeführt werden.

9.4.12 Vier-Augen-Prinzip (Confirmed Double Check Principle)

Beim Vier-Augen-Prinzip erfolgt durch Hinzuziehung einer zweiten Person eine gegenseitige Kontrolle und gemeinsame Übernahme der Verantwortung.

9.4.13 Prinzip der Funktionstrennung (Segregation of Duties)

Dieses Prinzip soll erreichen, dass Funktionen, die nicht miteinander vereinbar sind, getrennt sind, d. h. ein und dieselbe Person darf nicht beide Funktionen innehaben. Beispielsweise dürfen Personen einer genehmigenden oder einer prüfenden Funktion, wie z. B. die Revision, die Qualitätssicherung oder ein Testteam, nicht gleichzeitig auch der geprüften Funktion angehören.

Beispiele

Personen der Revision dürfen daher nicht der zu prüfenden Rechtsverwaltung (Administration) angehören, Mitglieder des Testteams oder der Produktion nicht in der Programmierung tätig sein. Umgekehrt formuliert fordert die Funktionstrennung somit eine Trennung von Entwicklung, Test und Produktion sowie Revision. Hierdurch können Interessenskonflikte vermieden werden.

Das Prinzip der Funktionstrennung sollte bereits in einer frühen Phase, z. B. während der Konzeption eines Informationssystems oder eines Rechenzentrums berücksichtigt werden. Dies ermöglicht es, Funktionalitäten oder Räumlichkeiten entsprechend den Anforderungen der Funktionstrennung vorzusehen.

9.4.14 Prinzip der Sicherheitsschalen (Security Shells)

Zu sichernde Werte sollten in Abhängigkeit von ihrem Schutzbedarf nur über mehrere Sicherheitsbarrieren erreichbar sein. Diese Sicherheitsbarrieren sollten die zu schützenden Werte wie Zwiebelschalen umgeben. Es entsteht das Schalenmodell aus Objekt-, Zufahrts-, Zutritts-, Zugangs-, Zugriffs- und Leseschutz.

In Abhängigkeit vom Schutzbedarf kann jede dieser Sicherheitsschalen für sich in weitere Schalen unterteilt sein oder eine unterschiedliche Stärke besitzen. Beispielsweise ist der Zutritt zum Gebäude eines Unternehmens durch ein Zutrittskontrollsystem in Form eines chipkartengesteuerten Drehkreuzes gesichert. Wer anschließend Zutritt zum hausinternen Rechenzentrum erhalten möchte, muss eine Vereinzelungsschleuse durchschreiten, die über Chipkarte und Fingerabdruck gesichert ist.

9.4.15 Prinzip der Pfadanalyse

Bei der Pfadanalyse wird das betrachtete Objekt in den Mittelpunkt gestellt und alle Pfade zu ihm im Hinblick auf Betriebs- und Angriffssicherheit analysiert. Bei Nutzung des Schalenmodells kann für jede Schale untersucht werden, ob alle Pfade zum Schutzobjekt auf vergleichbarem Sicherheitsniveau abgesichert sind. Zur Darstellung der Verbindungsstellen durch die einzelnen Sicherheitsschalen kann z. B. die Symbolik der Strukturierten Analyse verwendet werden, die von Tom DeMarco 1978 in seinem Buch „Structured Analysis and System Specification“ beschrieben wurde [24].

9.4.16 Prinzip des generellen Verbots (Deny All Principle)

Das Prinzip des generellen oder auch grundsätzlichen Verbots (Deny-All-Prinzip) besagt, dass alles verboten ist, was nicht explizit erlaubt ist.

Verbotsprinzip

9.4.17 Prinzip der minimalen Rechte (Need to Use Principle)

Das Prinzip der minimalen Rechte oder „need-to-use“-Prinzip dient dazu, Subjekten, z. B. Personen, nur die Rechte auf die Objekte zu geben, die sie zur Erfüllung ihrer Aufgaben mindestens benötigen. Das Prinzip der minimalen Rechte ist z. B. anwendbar auf Zufahrt, Zutritt, Zugang und Zugriff.

*Zufahrt,
Zutritt,
Zugang,
Zugriff*

Beispielsweise erhalten nur entsprechend autorisierte Personen das Recht, das Rechenzentrum, die Technikräume oder andere sicherheitsrelevante Räumlichkeiten zu betreten. Dieses Recht kann darüber hinaus noch genauer spezifiziert werden, indem diese Berechtigung nur für bestimmte Tageszeiten und Tage, z. B. Werktage, erteilt wird.

*Beispiel
Zutritts-
berechtigung*

Ähnliches gilt für den Zugang zu Systemen. Der Zugriff auf Daten wird durch entsprechende Rechte, z. B. Lesen, Schreiben, Löschen etc. näher festgelegt.

9.4.18 Prinzip der minimalen Dienste

Das Prinzip der minimalen Dienste besagt, dass den Nutzern (Personen, oder anderen (ITK-) Systeme) von Ressourcen nur die Dienste zur Verfügung gestellt werden, die sie tatsächlich benötigen. Bei Informationssystemen bedeutet dies, dass nur die Funktionalität angeboten wird, die erforderlich ist. Firewalls und aktive Netzkomponenten werden dementsprechend so konfiguriert, dass sie nur jene Dienste anbieten, die benötigt werden. Ähnliches gilt für die Nutzung von USB-Schnittstellen, Diskettenlaufwerken, entgeltspflichtige

Rufnummern von Mehrwertdiensten (in Deutschland: (0)900 9er-Nummern), Rufumleitung auf Handies, Roaming und Auslandstelefonaten.

9.4.19 Prinzip der minimalen Nutzung

Das Prinzip der minimalen Nutzung besagt, dass Nutzer (Personen oder andere Systeme) Ressourcen und Berechtigungen stets nur in dem Umfang nutzen dürfen, wie es Ihnen erlaubt ist. Dies bezieht sich beispielsweise auf Informations- und Kommunikationssysteme und Anlagen, aber auch auf Zufahrts-, Zutritts-, Zugangs- und Zugriffsrechte.

9.4.20 Prinzip der Nachvollziehbarkeit und Nachweisbarkeit

Alle sicherheitsrelevanten Aktivitäten, Ergebnisse und Ereignisse müssen im erforderlichen Umfang nachvollziehbar sein. Aufzeichnungen über sicherheitsrelevante Ereignisse dürfen nicht veränderbar sein.

9.4.21 Prinzip des „sachverständigen Dritten“

Das Prinzip des „sachverständigen Dritten“ dient als Orientierung für die Dokumentations- und Detaillierungstiefe. Es besagt, dass Dokumentationen stets so gestaltet sein sollten, dass ein sachverständiger, aber unternehmensfremder Dritter innerhalb eines vorgegebenen Zeitraums die angedachten Tätigkeiten durchführen kann, z. B. einen Plattentausch bei mehreren RAID-Arrays: Hierzu muss er beispielsweise wissen, welche Disks zu dem RAID-Array gehören und wie sicherheitskritisch das RAID-Array für den IT-Betrieb ist.

9.4.22 Prinzip des Closed-Shop-Betriebs und der Sicherheitszonen

Das Prinzip der Sicherheitszonen lässt sich auf unterschiedliche Themenstellungen anwenden. In der Folge wird es am Beispiel von Zutrittszonen, Netzsegmenten, Speicherbereichen und Brandabschnitten beschrieben.

Zutrittszonen

Der Bereich Informationsservices eines Unternehmens sollte die sicherheitskritischen IT-Produktionsbereiche bzw. den IT-Produktionsbetrieb abschotten und als „Closed-Shop“ betreiben. Den Produktionsbereich selber sollte der Leiter des IT-Betriebs bei Bedarf unterteilen in einzelne Sicherheitszonen, sodass eine gezielte Zutrittssteuerung möglich ist sowie die Bildung von Brandabschnitten. Separate Sicherheitszonen können beispielsweise eingerichtet werden für

den Großrechner, die Speichereinheiten, die Drucker, das Archiv und das Operating.

Die Unterteilung eines Gebäudes in Brandabschnitte erschwert Bränden die Ausbreitung und stellt eine Form von Sicherheitszonen dar.

Brandabschnitte

Eine Aufteilung nach Sicherheitszonen in Abhängigkeit von der Sicherheitsklassifikation empfiehlt sich auch für das Netz. Hier besteht die Möglichkeit, das physikalische Netz durch Switches in logische Netzsegmente, so genannte virtuelle LANs (VLAN) zu unterteilen.

*Logische
Netzsegmente*

Speicherbereiche des Computers sollte das Betriebssystem dynamisch in Zonen aufteilen und klassifizieren. Durch eine Kennzeichnung der Daten- und Programmbereiche des Speichers und dessen Verwaltung durch das Betriebssystem lassen sich Schreibvorgänge in den Programmbereich und Befehlsausführungen im Datenbereich verhindern. Speicherbereiche können also zu gegebener Zeit entweder beschrieben werden oder die dortigen Befehle ausgeführt werden, nicht aber beides. Diese Möglichkeit heißt „Write XOR Execute“.

*Speicherbereichs
zonen*

9.4.23 Prinzip der Prozess-, Ressourcen- und Lebenszyklus-immanenz

Damit Sicherheit ein integraler Bestandteil des Unternehmens ist, müssen in alle betroffenen Prozesse und Ressourcen des Unternehmens Sicherheitselemente integriert und in den Prozessen Sicherheitsaspekte berücksichtigt werden. Ist dies der Fall, so spreche ich von prozess- bzw. ressourcenimmanenter Sicherheit. Prozesse können dabei einen Ablauf beschreiben, welcher die Herstellung eines Produkts oder die Erbringung einer Dienstleistung beschreibt.

*Prozess- und
ressourcen-
immanente
Sicherheit*

Bevor diese Prozesse, deren Ressourcen, wie z. B. Systeme, sowie Produkte und Dienstleistungen genutzt werden, durchlaufen sie verschiedene Entwicklungsphasen von der Idee über die Konzeption und den Test bis hin zum Betrieb und zur Außerbetriebnahme, den Lebenszyklus. Ein klassisches Beispiel hierfür ist der Lebenszyklus von Software und IT-Systemen. Damit Prozesse und Systeme in der Phase des Betriebs und Produkte in der Nutzungsphase über die erforderlichen Sicherheitselemente und -merkmale verfügen, werden im gesamten Lebenszyklus Sicherheitsaspekte und Sicherheitselemente integriert. So wird eine lebenszyklusimmanente Sicherheit erreicht.

*Lebenszyklus-
immanente
Sicherheit*

Insgesamt ergibt sich so eine lebenszyklus-, prozess- und ressourcen-immanente Sicherheit [9], die sich in einer produkt- bzw. dienstleistungsimmanenten Sicherheit fortsetzt.

9.4.24 Prinzip der Konsolidierung

Durch die kontinuierliche Veränderung und Weiterentwicklung der Märkte, Prozesse und Technologien sind in angemessenen Zeitabständen Konsolidierungsmaßnahmen erforderlich. Ziel dieser Maßnahmen ist die Prüfung und anschließende Komplexitätsreduktion, um mehr Transparenz und weniger Fehlbedienungen zu erreichen sowie die Wirtschaftlichkeit zu erhöhen.

Der reduzierten Komplexität steht oftmals eine gesteigerte Abhängigkeit von der Sicherheit der eingesetzten konsolidierten Objekte gegenüber. Die Wirtschaftlichkeit nimmt durch Konsolidierung üblicherweise zu, nicht nur wegen Skaleneffekten, sondern auch durch ein geringeres vorzuhaltendes Know-how-Spektrum. Konsolidierungen beziehen sich auf Prozesse, verschiedene materielle und immaterielle Ressourcen sowie die Organisation, wie die folgende Auflistung zeigt:

1. Prozesse (Processware)
2. Technologien (Hardware, Software, Middleware)
3. Schnittstellen (Interfaces)
4. Daten (Dataware)
5. Wissen (Knowledgeware) und
6. Organisation (Orgware).

*Prozess-
konsolidierung*

Bei der Konsolidierung von Prozessen werden im Unternehmen vorhandene Prozesse mit gleichen Aufgabenstellungen ermittelt und vereinheitlicht. Hierzu gehören beispielsweise unterschiedliche Prozesse für das Projekt-, Qualitäts- und Sicherheitsmanagement einschließlich Kontinuitätsmanagement. Dies ermöglicht die Optimierung und Effizienzsteigerung der betroffenen Prozesse.

*Technologie-
konsolidierung*

Technologiekonsolidierung beschäftigt sich mit der Vereinheitlichung technologischer Komponenten. Beispiele hierfür sind die Server-, Netz- und Speicherkonsolidierung sowie die Konsolidierung von Betriebssystemen, Datenbanken und Anwendungen, z. B. für Textverarbeitung, Tabellenkalkulation und HTML-Seiten-Erstellung. Bei Anlagen, Systemen und Produkten können die verwendeten Komponenten konsolidiert werden.

*Schnittstellen-
konsolidierung
und
service-
orientierte
Architektur*

Schnittstellen zwischen Prozessen sowie zwischen Prozessen und Ressourcen sind oftmals durch Medienbrüche sowie fehlende oder unzureichende Standardisierung oder Abstimmung geprägt. Dies macht sie anfällig für Bedrohungen und Fehler und gefährdet dadurch Sicherheitskriterien, wie die Verfügbarkeit und Integrität. Technologischer Fortschritt und Standards ermöglichen die Konsolidierung der Schnittstellen durch Vermeidung von Medienbrüchen

und Vereinheitlichung der Schnittstellen. Hierdurch lassen sich gegebenenfalls zusätzlich Einsparungen erzielen.

Ein Beispiel für die Schnittstellenkonsolidierung ist die service-orientierte Architektur (Service Oriented Architecture {SOA}) [25]. Komplexe monolithische IT-Anwendungen werden hier ersetzt durch modulare Services mit standardisierten Schnittstellen.

Die Datenkonsolidierung beschäftigt sich damit, die im Laufe der Zeit an verschiedenen Stellen und in unterschiedlichen Anwendungen entstandenen Daten und Datenformate in geeigneter Form zusammenzuführen und zu speichern.

*Daten-
konsolidierung*

Bei der Wissenskonsolidierung gilt es, vorhandenes Wissen, das sich beispielsweise in unterschiedlichen Richtlinien, Regelwerken und Methoden äußert, oder nur in Köpfen vorhanden ist, zusammenzuführen und den Beteiligten verfügbar zu machen. Wissensdefizite lassen sich so verringern und sicherheitsrelevantes Know-how erhöhen.

*Wissens-
konsolidierung*

Die Organisationskonsolidierung ergibt sich aus den Folgen von Veränderungen in Märkten, Prozessen und Technologien. Beispiele hierfür sind Fusionen, Kooperationen und Auslagerungen bis hin zum Business Process Outsourcing. Diesen Entscheidungen liegen in der Regel strategische und finanzielle Überlegungen zugrunde.

*Organisations-
konsolidierung*

9.4.25 Prinzip der Standardisierung (Principle of Standardization)

Je mehr unterschiedliche Abläufe und Hilfsmittel ein Unternehmen bzw. der Bereich Informationsservices einsetzt, desto aufwändiger ist die Schulung der Mitarbeiter, desto komplexer und intransparenter wird die ITK und desto leichter können Fehler passieren. Um dem entgegenzuwirken, sollte die der Bereich Informationsservices seine Abläufe und Hilfsmittel standardisieren.

Bei Informationssystemen bedeutet dies, dass es rollenspezifisch standardisierte PC-Ausstattungsvarianten gibt und dass alle PCs z. B. den gleichen Browser erhalten. Hierdurch müssen Benutzer und Administration nur für diesen Browser geschult werden. Administratoren müssen Sicherheitspatches nur für diesen Browser einspielen, gegebenenfalls sind auch die Lizenzkosten aufgrund der größeren Anzahl der Nutzer günstiger.

9.4.26 Prinzip der Plausibilisierung (Principle of Plausibleness)

Schnittstellen jeglicher Art stellen potenzielle Fehlerquellen dar und bieten Angriffspunkte. Derartige Schnittstellen befinden sich beispielsweise innerhalb eines Schutzobjektes oder zwischen Schutzob-

jekten, z. B. zwischen Systemen und Anwendung sowie zu angrenzenden Systemen und Anwendungen. Um diese abzusichern, plausibilisieren Systeme die Daten, die sie von diesen Schnittstellen bekommen. Hierzu prüfen sie beispielsweise, ob die Eingabewerte das richtige Format einschließlich der erwarteten Länge besitzen und im zulässigen Wertebereich liegen.

Auf diese Weise lassen sich unbeabsichtigte Eingabefehler berechtigter Benutzer ebenso abfangen wie absichtliche Fehleingaben unrechtmäßiger Dritter, z. B. in Form von SQL-Injections. Das Prinzip der Plausibilisierung findet darüber hinaus Anwendung z. B. bei der Überprüfung des Kommunikationsflusses. Ein so ausgestattetes System prüft, ob eingehende Datenpakete von einem Absender stammen, mit dem eine Kommunikationsbeziehung besteht, ob das Datenpaket das richtige Format hat, ob es im Kommunikationsablauf zulässig ist, etc.

9.4.27 Prinzip der Konsistenz (Principle of Consistency)

Die Überprüfung der Konsistenz, z. B. zwischen Eingangs- und Ausgangsdaten oder eingegangenen, gespeicherten und versandten Daten ist ein weiteres Sicherheitsprinzip, das Prinzip der Konsistenz. Telekommunikationsunternehmen beispielsweise erhalten eine Vielzahl von Abrechnungsdaten aus ihren technischen Systemen, die sie den verschiedenen Kunden verursachergerecht zuordnen und nach unterschiedlichen Tarifen abrechnen. Die Zahl der abzurechnenden Einheiten sollte hierbei mit der Zahl der tatsächlich abgerechneten Einheiten übereinstimmen, also konsistent zueinander sein.

Ähnlich verhält es sich bei Banken mit eingehenden Finanztransaktionen, die in ihrer Summe ordnungsgemäß verbucht sein wollen. In Produktion und Fertigung sollten eingehende Materialien und Komponenten in einer entsprechenden Anzahl von Produkten münden, wobei eventueller Ausschuss zu berücksichtigen ist. Das Prinzip der Konsistenz ist – ähnlich dem Energieerhaltungssatz – sozusagen ebenfalls ein „Erhaltungssatz“.

9.4.28 Prinzip der Untergliederung (Principle of Compartmentalization)

Das Prinzip der Untergliederung bzw. Unterteilung dient dazu, die Sicherheit eines Schutzobjekts zu erhöhen. Hierzu zerlegen die Zuständigen das jeweilige Schutzobjekt in einzelne Komponenten, für die sie separate Schutzmaßnahmen vorsehen. Ein erfolgreicher Angriff auf eine Komponente betrifft dann nicht das Gesamtsystem und

kann dadurch gezielter behandelt werden. Gleichzeitig lassen sich so die Auswirkungen begrenzen.

Das Prinzip ist weitgehend identisch mit dem Prinzip der Sicherheitszonen, indem das Rechenzentrum beispielsweise unterteilt wird in separate Sicherheitszonen für den Großrechner, die Speichereinheiten, die Drucker, das Archiv und das Operating. Ein Angreifer gelangt so stets nur zu einem Teil der Schutzobjekte. Die Unterteilung in Sicherheitszonen lässt sich außerdem zum Schutz gegen Brand etc. verwenden.

9.4.29 Prinzip der Vielfältigkeit (Principle of Diversity)

Das Prinzip der Vielfältigkeit setzt auf voneinander unabhängige und verschiedenartige Sicherheitsmaßnahmen statt auf eine sehr mächtige. Dadurch muss ein Angreifer nicht nur eine, sondern mehrere Hürden mit unterschiedlichen Technologien überwinden, um an sein Ziel zu gelangen.

9.5 Sicherheitselemente

Bisher wurden die prinzipiellen Sicherheitsanforderungen und Bedrohungen sowie die Sicherheitsprinzipien und -strategien zusammengestellt. Im nächsten Schritt werden hierfür Sicherheitselemente entwickelt, welche die Bausteine der Sicherheitsarchitektur bilden.

Die Sicherheitselemente sollen zum einen die Betriebssicherheit (Safety), d. h. den sicheren und ordnungsmäßigen Betrieb der Informations- und Kommunikationssysteme, sowie die Kontinuität (Continuity) entsprechend den Anforderungen fördern. Optimal wäre hier das Wort „sicherstellen“ anstelle von „fördern“. Dies ist jedoch nicht angebracht, denn 100 %ige Sicherheit gibt es nicht und die letzten Prozente auf dem Weg zu ihr sind erfahrungsgemäß die teuersten.

*Betriebs-
sicherheit,
Ordnungs-
mäßigkeit,
kontinuierliche
Verfügbarkeit*

Zum anderen haben die Sicherheitselemente die Aufgabe, vor kriminellen Handlungen sowie böswilligen internen und externen Angriffen zu schützen, d. h. die Angriffssicherheit (Security) zu erhöhen.

*Angriffs-
sicherheit*

Die Sicherheitselemente sind in der Architektur überblicks- und schlagwortartig dargestellt. Es gibt sie für jedes Themen-Cluster in PROSim. Prozesse, u. a. für das Security-, Kontinuitäts- und Datenschutzmanagement, sowie die Unterthemen wie Identifikation und Authentisierung, Datensicherung und Katastrophenvorsorge, sind Beispiele für Sicherheitselemente.

*Sicherheits-
elemente*

Jedes Sicherheitselement, das in der Architektur im ersten Schritt schlagwortartig angeführt ist, wird in der Folge verfeinert und detail-

liert beschrieben. Für das Sicherheitselement Datensicherung müssen beispielsweise der Prozess der Datensicherung, die genutzten Ressourcen in Form von Technologien, Materialien (z. B. Datenträger) und Methoden, die personelle Qualifikation und erforderliche Kapazität sowie die organisatorische Verantwortlichkeit für die Datensicherung festgelegt werden.

*Anforderungs-
spezifische
Auswahl der
Sicherheits-
elemente*

In Abhängigkeit von den Sicherheitsanforderungen eines Schutzobjekts, z. B. eines ITK-Systems, werden die prinzipiellen Sicherheitselemente, die in der Sicherheitsarchitektur definiert sind, aktiviert, d. h. genutzt, oder nicht. Daher enthält die Sicherheitsarchitektur alle Elemente, die zur Erreichung des höchsten geforderten Sicherheitsniveaus erforderlich sind. Bei Nutzung vordefinierter Sicherheitsklassen sind Standardzuordnungen zwischen Sicherheitsklasse und erforderlichen Sicherheitselementen möglich. Dies vereinfacht und vereinheitlicht das weitere Vorgehen je Schutzobjekt und macht es effizienter.

Die jeweilige konkrete aktuelle Ausprägung der PROSim-basierenden unternehmensspezifischen Sicherheitsarchitekturfelder findet sich beispielsweise in der Prozess- und der Anwendungsarchitektur sowie der Netztopologie wieder. Entsprechen diese nicht den Zielvorstellungen, so bilden sie den Ausgangspunkt zur Entwicklung einer Strategie und eines Migrationsplans zur Erreichung des Zielzustands.

*Weitere
Gliederungs-
struktur des
Kapitels*

Entsprechend PROSim sind die folgenden Unterkapitel gegliedert in die Überblicke über Prozesse, Ressourcen und Organisation sowie den Lebenszyklus. Aufgrund der Bedeutung der Prozesse und zur leichteren Auffindbarkeit im nur vierstufigen Inhaltsverzeichnis habe ich in der Kapiteluntergliederung ein wenig „geschummelt“. Sie finden daher hinter dem Unterkapitel mit dem Überblick über Prozesse, aber auf der gleichen Kapitelebene, die verschiedenen Begleitprozesse bzw. Managementdisziplinen. Erst anschließend folgen die Überblickskapitel für Ressourcen und Organisation sowie das Kapitel zum Lebenszyklus.

9.5.1 Prozesse im Überblick

*Kern- und
Supportprozesse*

Jedes Unternehmen hat einen Zweck, d. h. eine Mission. Um den Unternehmenszweck zu erreichen, sind Kernprozesse erforderlich. Diese beschreiben, wie beispielsweise Produkte hergestellt oder Leistungen erbracht werden. Die Kernprozesse nutzen zur Leistungserbringung gegebenenfalls Unterstützungsprozesse (Supportprozessen). Das Facility Management ist ein solcher Supportprozess, aber auch der ITK-Betriebsprozess bzw. die ITK-Produktion, die den Be-

triebsprozess der Informations- und Telekommunikationssysteme beschreiben.

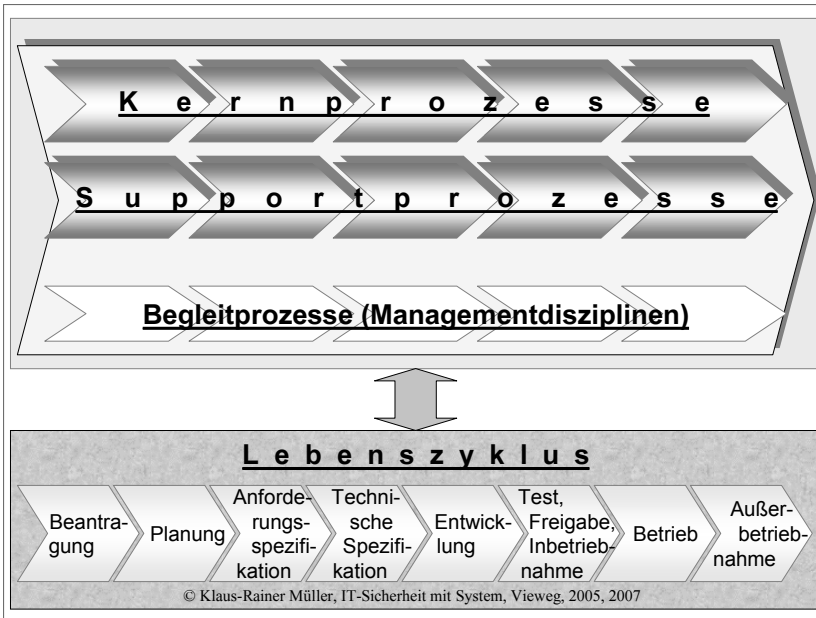


Abb. 9.2: Kern-, Support- und Begleitprozesse im Lebenszyklus

Parallel zu den Kern- und Unterstützungsprozessen sind Begleitprozesse erforderlich. Diese werden auch als Managementdisziplinen bezeichnet. Die Begleitprozesse berücksichtigen u. a. die kontinuierlichen Veränderungen der Prozesse und der von ihnen genutzten Ressourcen. Zu den Begleitprozessen gehören u. a. das Konformitäts-, Datenschutz-, Kapazitäts-, Änderungs- und Konfigurationsmanagement.

*Begleitprozesse,
Management-
disziplinen*

Die bisherigen Darstellungen dieses Kapitels bezogen sich auf die Phase des Betriebs eines Prozesses. Wie wir in vorangegangenen Kapiteln gesehen haben, sind für einen sicheren Betrieb jedoch bereits ab dem Beginn des Lebenszyklus eines jeden Prozesses, sei es ein Kern-, Support- oder Begleitprozess, Sicherheitsaspekte und Sicherheitselemente zu berücksichtigen. Zusätzlich dazu, dass die Begleitprozesse selbst einen Lebenszyklus besitzen, erstrecken sie sich dementsprechend auch über den gesamten Lebenszyklus anderer Prozesse sowie über den Lebenszyklus von Ressourcen, Dienstleistungen (Services) und Produkten. Durch die Integration von Sicherheitsele-

*Lebenszyklus
und
lebenszyklus-
immanente
Sicherheit*

menten in den Lebenszyklus lässt sich eine lebenszyklusimmanente Sicherheit erreichen.

*Folgende
Unterkapitel*

Die beiden folgenden Unterkapitel geben Ihnen einen Überblick zum einen über die Kern- und Supportprozesse und zum anderen über die Begleitprozesse bzw. Managementdisziplinen. Die Bezeichnung Managementdisziplin verdeutlicht, dass in ihr bestimmte Aufgabenstellungen zu planen, zu verwalten, zu überwachen und zu steuern sowie durch einen Prozess zu regeln sind. In allen Prozessen ist dabei darauf zu achten, dass sie externe Anforderungen berücksichtigen, wie sie u. a. hinsichtlich Ordnungsmäßigkeit, Arbeitssicherheit, Archivierung, Datensicherung und Notfallvorsorgeplanung existieren. Außerdem ist das Thema Marktbeobachtung für alle Prozesse relevant.

9.5.1.1 Kern- und Unterstützungsprozesse im Überblick

Einen ersten Überblick über die Kern- und Unterstützungsprozesse (Supportprozesse) sowie deren Zusammenspiel gibt die bereits früher erwähnte Prozessarchitektur. Kernprozesse sind auf den Kunden ausgerichtet. Supportprozesse und ihre Ressourcen unterstützen die Kernprozesse. Sie sind in der Regel für den Geschäftsbetrieb erforderlich, stabil und in verschiedenen Unternehmen prinzipiell gleich, wie z. B. das Human Resources Management bis hin zur Gehaltsabrechnung, die Buchführung oder das Management der ITK.

*Sicherheits-
merkmale*

Der Schutzbedarf jedes einzelnen Prozesses bestimmt, welche Sicherheitsmerkmale er erhält. So sichert beispielsweise das Vier-Augen-Prinzip und die Funktionstrennung sicherheitskritische Stellen in Prozessen ebenso ab, wie Vollmachtenregelungen und Rechtekonzepte. Zu den Rechten gehören beispielsweise Zutrittsrechte zu Räumlichkeiten, Zugangsrechte zu Anwendungen sowie Zugriffsrechte auf Daten, Dokumente und Informationen.

*ITK-Betriebs-
prozess*

Im ITK-Bereich ist insbesondere daran zu denken, dass der Betrieb von Informations- und Kommunikationssystemen nicht nur Anforderungen an die Sicherheit der eingesetzten Systeme stellt, sondern auch an die dazugehörigen Prozesse. So bedeutet die Hochverfügbarkeit eines Systems zum einen dessen anforderungsgerechte Redundanz und die Redundanz der von ihm genutzten Ressourcen, wie z. B. der Stromversorgung. Zum anderen müssen die ITK-Betriebsprozesse dementsprechend abgesichert sein, so dass ein Ausfall von Personal, Gebäude oder genutzten Ressourcen, wie z. B. Steuerungswerkzeugen, nicht zu einer Betriebsunterbrechung führt.

Zum ITK-Betriebsprozess gehört u. a. das Monitoring, Erkennen, Aufzeichnen (logging), Auswerten und Melden von Ereignissen, das Alarmieren sowie die Steuerung der ITK und das Reporting. Dies schließt sicherheitsrelevante Ereignisse ein. Weitere Aktivitäten bestehen beispielsweise in der Installation, Deinstallation, Konfiguration, Aktivierung und Deaktivierung von Komponenten (Managed Objects), im Sichern und Rückspeichern von Daten, in der Datenbank-Administration und –Reorganisation, in der Durchführung von Konfigurationsänderungen und Tuning-Maßnahmen, in der Lastverteilung, in der Planung (scheduling) und Durchführung von Batch-Verarbeitungsläufen und Datensicherungen sowie in der Überwachung und Steuerung der CPU-, Netz-, Speicher- und Drucker-Auslastung.

9.5.1.2 Begleitprozesse (Managementdisziplinen) im Überblick

Im Folgenden finden Sie einen Überblick über die Begleitprozesse der Kern- und Unterstützungsprozesse. In den anschließenden Einzelkapiteln sind die Begleitprozesse detaillierter erläutert. Zu beachten ist, dass sowohl diese Prozesse als auch die von ihnen genutzten Ressourcen, wie z. B. Überwachungstools, Sicherheitsanforderungen unterliegen. Diese Sicherheitsanforderungen leiten sich aus den dazugehörigen Kern- und Supportprozessen ab.

Bei den Begleitprozessen machen sich die Größenunterschiede von Unternehmen meist besonders bemerkbar. Während bei Großunternehmen jeder einzelne Begleitprozess aufgrund seiner Komplexität, der Vielzahl der Beteiligten und der verteilten Verantwortlichkeiten umfangreich beschrieben ist, kann er bei kleinen Unternehmen aus wenigen knapp gefassten Aufgaben und Checklisten bestehen. Das dementsprechende angemessene Komprimieren dieser Managementdisziplinen erscheint mir sinnvoll und zielführend, sie wegzulassen nicht. Letzteres führt zu leicht zu Defiziten, die die Handlungsfähigkeit des Unternehmens gefährden können.

Welche Begleitprozesse gibt es nun? Ausgangspunkt für die sicherheitsspezifische Gestaltung von Prozessen, Ressourcen, Produkten und Dienstleistungen sind gesetzliche, vergleichbare und vertragliche Anforderungen, die für das Unternehmen und seine ITK gelten. Häufig spielen sicherheitsrelevante Anforderungen des Handelsgesetzbuches (HGB), des Aktiengesetzes (AktG) einschließlich der Elemente des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und des Urheberrechts (Lizenzen, Darstellungen) eine wesentliche Rolle. Darüber hinaus gibt es Gesetze und Regelungen, die branchenspezifisch berücksichtigt werden müssen, wie z. B.

*Konformitäts-
(Compliance-)
management*

bei Gesetzlichen Krankenversicherungen das Sozialgesetzbuch (SGB) mit dem Schutz der Sozialdaten, oder bei Banken das Bankgeheimnis und das Meldewesen. Der Prozess des Konformitätsmanagements hat die Aufgabe, die Kenntnis, Aktualität und Erfüllung (compliance) dieser Anforderungen sicherzustellen.

Datenschutz- management

Der Datenschutz in Form der Datenschutzgesetze, wie z. B. des Bundesdatenschutzgesetzes (BDSG), besitzt einen besonderen Stellenwert und erfordert spezifische Verantwortlichkeiten. Dies bildet der Begleitprozess Datenschutzmanagement ab.

Risiko- management

Mit dem Betrieb eines Unternehmens sowie der Erfüllung gesetzlicher, vertraglicher und unternehmensspezifischer Anforderungen gehen Risiken einher. In der Risikopolitik legt das Unternehmen seine Risikobereitschaft fest und definiert, welche Risiken noch tragbar sind und welche abgesichert werden müssen. Darauf aufbauend gilt es, Risiken zu identifizieren, zu analysieren, zu bewerten und zu steuern. Hierzu ist ein Prozess erforderlich, das Risikomanagement.

Leistungs- management

Ausgangspunkt für die Gestaltung von ITK-Systemen sind die Anforderungen der Nutzer. Sie bilden die Grundlage für die Leistungsvereinbarungen (Service Level Agreements) und müssen im Rahmen der Aufbewahrungsfristen jederzeit in ihrem aktuellen Stand und in ihrer Historie nachvollziehbar verfügbar sein. Ihnen gegenüber stehen die tatsächlich erbrachten Leistungen. Die Verwaltung, Verfolgung, Überwachung und Steuerung der Leistungsvereinbarungen und -erbringung erfolgt durch das Leistungsmanagement (Service Level Management).

Dienstleister- management

In die Erbringung dieser Leistungen sind meist interne und oftmals auch externe Auftragnehmer eingebunden. Die Vereinbarungen mit den internen Dienstleistern sowie mit den externen müssen durch das interne Leistungsmanagement sowie das Dienstleistermanagement, das Teil des Leistungsmanagements ist, verwaltet und gesteuert werden. Hierzu gehört auch das Management eventuell abgeschlossener Versicherungen.

Finanz- management

Für die selbst zu erbringenden und die eingekauften Leistungen sowie für deren Absicherung stehen die mit den Kunden vereinbarten finanziellen Mittel bereit. Diese müssen erfasst, eingeplant und durch ein entsprechendes Controlling verfolgt und gesteuert werden. Dies ist Aufgabe des Finanzmanagements.

Projekt- und Qualitäts- management

Für die Sicherheit entscheidend ist die fehlerfreie Funktionsfähigkeit aller Systemkomponenten im Betrieb. Dies erfordert ein ausgereiftes Projekt- und Qualitätsmanagement über alle Phasen des Lebenszyklus.

Informationssysteme sind meist hoch komplex. In der Betriebsphase treten daher erfahrungsgemäß Ereignisse auf, die den regulären Betrieb und damit z. B. die Ordnungsmäßigkeit und Verfügbarkeit stören. Sie sind u. a. auf Fehlbedienungen, technische Defekte oder Fehlfunktionen zurückzuführen. Die Entgegennahme derartiger Ereignisse, seien es Fragen, Schwierigkeiten, Störungen oder Probleme, und deren möglichst sofortige Lösung erfolgt häufig durch eine zentrale Anlaufstelle („Single Point of Contact“), das User Help Desk (UHD).

*Ereignis- und
Problem-
management*

Dieses nutzt zur Ereignisbearbeitung den Prozess Ereignismanagement. Ziel dieses Prozesses ist die kurzfristige Unterstützung bei Fragen oder Schwierigkeiten sowie die Lösung von Störungen, z. B. durch eine Umgehung (workaround) oder das Rücksetzen (reset) und den Neustart (restart) eines Informationssystems, PCs oder Druckers. Demgegenüber konzentriert sich das Problemmanagement neben der Entgegennahme und Verfolgung primär auf die ursachenorientierte und damit endgültige Behebung von Problemen, um die Qualität und Sicherheit zu steigern.

Insbesondere die Informationsverarbeitung unterliegt einem kontinuierlichen Wandel und kurzen Veränderungszyklen. Prozesse werden geändert und standardisiert, Schwachstellen erkannt, gemeldet und sollen behoben werden, zugrundeliegende Technologien verändern sich und erfordern einen Austausch. Der heute gekaufte PC, das heute gekaufte Betriebssystem, die heute gekaufte Anwendung ist „morgen“ schon veraltet. Diese Veränderungen müssen verfolgt und hinsichtlich der Auswirkungen auf das eigene Unternehmen und die ITK bewertet werden. Sie führen auf Seiten der Kunden und auch der Anwender oftmals zu neuen Anforderungen.

*Kurze
Veränderungs-
zyklen*

Aus dem Problemmanagement resultieren Änderungsanforderungen für die Behebung von Fehlern und Schwachstellen, z. B. für Prozesse oder ITK-Systeme. Aber auch technologische Änderungen und Neuentwicklungen aufgrund neuer Kundenanforderungen führen zu Änderungsanforderungen (change request) an bestehenden Systemen und Systemlandschaften. Diese Änderungen müssen dokumentiert, priorisiert, geplant und verfolgt sowie ihre potenziellen Risiken im Vorfeld untersucht und abgesichert werden. Erst dann sollten Fehler behoben, Software-Patches eingespielt, Software-Updates vorgenommen und Systemkomponenten oder ganze Systeme ausgetauscht werden. Hierzu dient das Änderungsmanagement.

*Änderungs-
management*

Die Bündelung von Änderungen zu Releases sowie das Verfahren und die Steuerung zur Einführung neuer Releasestände beschreibt das Releasemanagement.

*Release-
management*

<i>Konfigurationsmanagement</i>	Aufgrund der vielfältigen Änderungen geht schnell der Überblick verloren, in welcher Konfiguration aus Patch-Leveln und Release-Ständen der einzelnen Komponenten sich ein Informationssystem befindet. Um dem entgegenzusteuern, ist das Konfigurationsmanagement erforderlich. Es verschafft den Überblick über aktuelle und frühere Konfigurationen von Prozessen und Ressourcen, wie z. B. Systemen und Dokumenten, sowie Produkten. So unterstützt es die zügige und zielgerichtete Bearbeitung von Störungen oder Problemen.
<i>Lizenzmanagement</i>	Für den ordnungsmäßigen ITK-Betrieb ist sicherzustellen, dass für jene Systeme und Verfahren, die lizenzrechtlichen Bestimmungen unterliegen, die erforderlichen Lizenzen vorhanden sind. Der dazugehörige Prozess heißt Lizenzmanagement.
<i>Kapazitätsmanagement</i>	Änderungen und funktionale Erweiterungen der Software, aber auch die reguläre Nutzung durch die Anwender führen in der Regel zu einer Zunahme der Datenbestände und der CPU-Belastung. Dies zusammen mit einer steigenden Anzahl der Nutzer kann sich auf die Performance auswirken und zu Kapazitätsengpässen führen. Diese Entwicklung muss beobachtet und die Kapazität der Systeme rechtzeitig geplant und angepasst werden. Diese Aufgaben erfüllt das Kapazitätsmanagement.
<i>Kontinuitätsmanagement</i>	Alle diese Managementdisziplinen sind Bausteine für einen sicheren Betrieb der ITK unter primär störungsfreien Bedingungen („Schönwetterflug“). Doch was passiert in Notfällen, wie z. B. dem Ausfall geschäftskritischer Ressourcen, die ja zum Arbeitsalltag gehören? Diese müssen durch das Kontinuitätsmanagement den jeweiligen Anforderungen entsprechend angemessen abgesichert werden.
<i>Securitymanagement</i>	Die bisher genannten Begleitprozesse konzentrierten sich auf die Betriebssicherheit, d. h. den regulären Betrieb und dessen Absicherung. Nun gilt es, sich vor kriminellen Handlungen, wie Diebstahl, Ressourcenmissbrauch und Spionage, sowie böswilligen Angriffen zu schützen. Spätestens das Internet hat hier zu einem weltumspannenden Angriffspotenzial geführt. Mit diesen Themen beschäftigt sich das Securitymanagement. Dessen Anforderungen beeinflussen die Begleitprozesse.
<i>Architekturmanagement</i>	Damit Unternehmen mit den Umfeldveränderungen Schritt halten können, sollte ihre Sicherheitsarchitektur kontinuierlich angepasst und weiterentwickelt werden. Hierzu dient das Architekturmanagement.
<i>Innovationsmanagement</i>	Märkte und Technologien verändern sich kontinuierlich. Dies hat Auswirkungen auf das Unternehmen und seine Prozesse. Die Chan-

cen und Risiken derartiger Innovationen rechtzeitig zu erkennen, zu bewerten und Maßnahmen zu ergreifen, ist Aufgabe des Innovationsmanagements.

Um den ITK-Betrieb einschließlich Entwicklung und Wartung aufrecht halten zu können, sind Personen erforderlich. Diese müssen – auch unter Sicherheitsaspekten – ausgewählt und betreut werden. Die hieraus resultierenden Sicherheitsanforderungen müssen im Personalmanagement berücksichtigt werden.

*Personal-
management*

Aus den vorangegangenen Schilderungen ergibt sich der Bedarf an folgenden Begleitprozessen bzw. Managementdisziplinen:

- Konformitätsmanagement (Compliance Management)
- Datenschutzmanagement (Privacy Management)
- Risikomanagement (Risk Management)
- Leistungsmanagement (Service Level Management)
- Finanzmanagement (Financial Management)
- Projektmanagement (Project Management)
- Qualitätsmanagement (Quality Management)
- Ereignismanagement (Incident Management)
- Problemmanagement (Problem Management)
- Änderungsmanagement (Change Management)
(einschließlich Patchmanagement)
- Releasemanagement (Release Management)
- Konfigurationsmanagement (Configuration Management)
- Lizenzmanagement (Licence Management)
- Kapazitätsmanagement (Capacity Management)
(Rechnermanagement, Speichermanagement
{Speicherhierarchie, -medien, -topologie})
- Wartungsmanagement (Maintenance Management)
- Kontinuitätsmanagement (Continuity Management)
(Prävention, Datensicherung, Notfall- und Katastrophenvorsorge,
Versicherung)
- Securitymanagement (Security Management)
(Rechtevergabe, -dokumentation, -steuerung, -verwaltung, Identifikation und Authentisierung {Token, Single Sign-on, Identitätsmanagement}, Zufahrts-, Zutritts-, Zugangsschutz, Zugriffs-, Leseschutz {Verschlüsselung}, Wiederaufbereitung, Absendekontrolle, Übertragungssicherung, Abgangskontrolle, Transportsicherung,

Abfahrtskontrolle, Meldung, Alarmierung, Protokollierung, Beweissicherung, Protokollauswertung, Berichtswesen)

- Architekturmanagement (Architecture Management)
- Innovationsmanagement (Innovation Management)
- Personalmanagement (Human Resources Management).

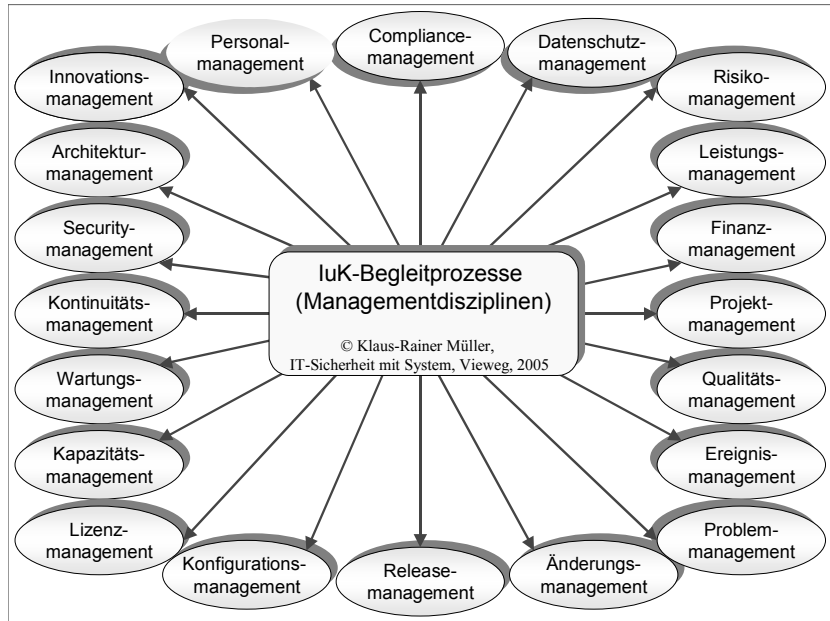


Abb. 9.3: Begleitprozesse (Managementdisziplinen)

IT
Infrastructure
Library (ITIL®)

Wem die IT Infrastructure Library (ITIL®) des Office of Government Commerce (OGC) bekannt ist, der findet zwischen den hier genannten Managementdisziplinen und den dortigen Parallelen, ebenso wie zur ISO 20000. Dies ist insofern nachvollziehbar, als ITIL® Best Practices beschreibt.

ITIL®, Version 2, fasst verschiedene Managementdisziplinen zu den Oberbegriffen Service Support und Service Delivery zusammen. Service Support umfasst die operativen Managementdisziplinen Change, Configuration, Release, Incident und Problem Management sowie die Funktion Service Desk. Service Delivery beinhaltet die taktischen Managementdisziplinen Financial, Service Level, Capacity, Availability und IT Service Continuity Management. Weitere Oberbegriffe sind Security Management, Infrastructure Management und Applications Management.

ITIL®, Version 2, unterscheidet zwischen Availability Management und IT Service Continuity Management (ITSCM). Das Availability Management beschäftigt sich hierbei mit der Planung, Implementierung, Messung und dem Management der IT-Services, so dass die Verfügbarkeitsanforderungen erfüllt werden. Es umfasst u. a. auch die Wartbarkeit und Zuverlässigkeit. ITSCM fokussiert sich demgegenüber darauf, vorgegebene minimale Geschäftsanforderungen nach einer Geschäftsunterbrechung bzw. einer größeren Katastrophe aufrecht erhalten zu können. Hierzu gehört der Wiederanlauf (recovery) IT-technischer Komponenten und Dienste innerhalb zuvor vereinbarter Zeiträume.

Die zuvor genannten Begleitprozesse bzw. Managementdisziplinen der Sicherheitspyramide begleiten den gesamten Lebenszyklus von Prozessen, Ressourcen, z. B. Informationssystemen, Produkten und Dienstleistungen (services). Sie sind Elemente der Prozessarchitektur zur Betriebs- und Angriffssicherheit.

*Prozess-
architektur*

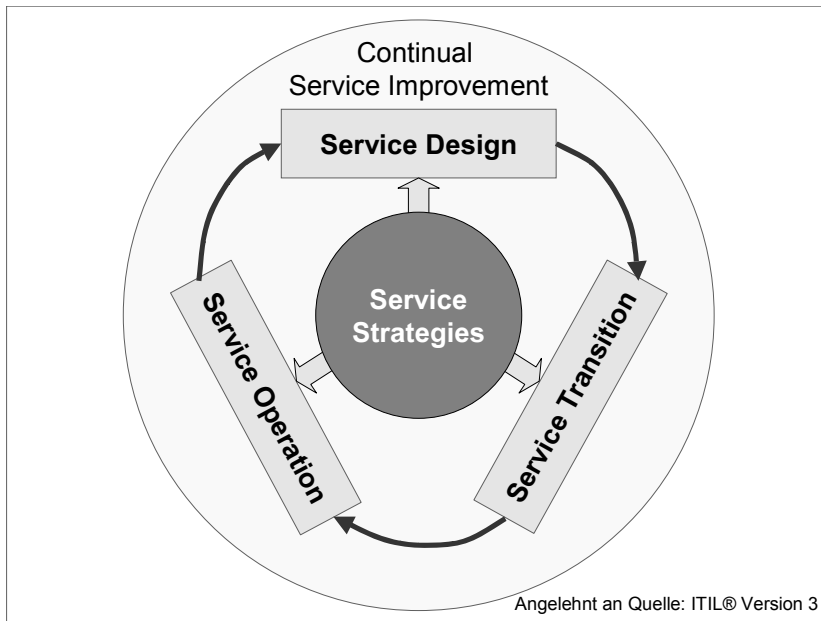


Abb. 9.4: ITIL® Service Life Cycle

ITIL® hat das Thema Lebenszyklus hinsichtlich der IT-Services erkannt und im Jahr 2007 in der Version 3 von ITIL® in Form des IT Service Lifecycle aufgegriffen. Das neue ITIL®-Modell ist damit nicht mehr prozess-, sondern lebenszyklusbasiert und zwar bezogen auf

IT-Services. Service Support und Service Delivery sind dementsprechend in das Lebenszyklusmodell integriert.

ITIL[®] V3 (s. a. [26], [27], [28]) besteht aus insgesamt 5 Titeln, die jeweils die gleiche Struktur aufweisen. Die ITIL[®]-V3-Werke haben eine neue Darstellung bekommen, die einem Rad ähnelt, das eine Nabe, Speichen und eine Felge besitzt. Das Kernelement bildet die Service Strategy. Sie ist verbunden mit den ineinandergreifenden Titeln Service Design, Service Transition und Service Operation. Continual Service Improvement (CSI) umrahmt diese Titel.

Service Strategy und Continual Service Improvement sind weitgehend neue Elemente. Die bisherigen ITIL[®]-Bücher der Version 2 finden ihren Niederschlag vorrangig in Service Design (SD), Service Transition (ST) und Service Operation (SO). SD enthält planerische Elemente der Service-Delivery-Prozesse. Hier gehen insbesondere die Prozesse Information Security Management, Service Continuity Management, Availability Management, Service Level Management und Capacity Management sowie Supplier Management ein. Das Thema Sourcing in Form von Out-, In- und Cosourcing ist ein weiteres Thema.

In ST finden sich Teile aus dem Change und Release Management sowie das Service Asset Management und das Knowledge Management. SO enthält viele Teile aus Service Support sowie die messungsrelevanten Teile der Begleitprozesse aus Service Delivery. Ferner behandelt SO die Themen Application Management, Infrastructure Management und IT Operations Management.

Prozesse Je nach Größe definieren Unternehmen die Begleitprozesse der Sicherheitspyramide in Form eigener Prozesse oder als integrale Bestandteile des Lebenszyklus. Die Prozesse erhalten entsprechende Verbindungsstellen untereinander und zum Lebenszyklus, um einen ausreichenden Informationsfluss zu erreichen. Die Prozesse werden im Hinblick auf die verschiedenen Sicherheitskriterien klassifiziert. Die Verfügbarkeitsklasse eines Prozesses beispielsweise hängt von seiner Bedeutung zur Erfüllung der Service-Vereinbarungen ab.

Aktivitäten In den verschiedenen Prozessen sind Aktivitäten zu definieren. Beispielsweise muss der Kapazitätsbedarf geplant und verfolgt oder die Konfiguration der Systeme aktuell gehalten werden.

*Ressourcen,
Schutzobjekte* Für die Prozessschritte sind Ressourcen bzw. Schutzobjekte erforderlich, wie z. B. Gebäude und Räumlichkeiten, Infrastruktur, Informationssysteme und Hilfsmittel bzw. Werkzeuge. Diese werden beim jeweiligen Prozessschritt definiert und in der Ressourcen-Architektur

abgebildet. Die Schutzobjekte werden ebenfalls im Hinblick auf die Sicherheitskriterien klassifiziert.

Die Aktivitäten müssen von Personen wahrgenommen und in der Organisation abgebildet werden. Um je Aktivität eine direkte namentliche Zuordnung mit den entsprechend häufigen Änderungen zu vermeiden, sollten Sie Aktivitäten zu Rollen zusammenfassen und schließlich in einer zentralen Rollen-Mitarbeiter-Matrix Mitarbeitern zuordnen. Für die Aktivitäten des Konfigurationsmanagements beispielsweise entsteht so die Rolle des Konfigurationsmanagers und seines Stellvertreters.

*Rollen,
Organisation*

Der Umfang und die Zeitintensität für die Aktivitäten in den Prozessen korrelieren oftmals mit der Unternehmensgröße. Dementsprechend kann ein Mitarbeiter bei einem kleineren Unternehmen mehrere Rollen wahrnehmen, während eine Rolle in einem größeren Unternehmen auf mehrere Mitarbeiter verteilt wird.

*Rollen-
zuordnung zu
Personal*

9.5.2 Konformitätsmanagement (Compliance Management)

Die Kenntnis und Einhaltung gesetzlicher, aufsichtsbehördlicher und vergleichbarer sowie normativer und vertraglicher Vorgaben ist Ausgangspunkt für die sicherheitsspezifische Gestaltung von Prozessen, Ressourcen, Produkten und Dienstleistungen. Der Prozess des Konformitätsmanagements hat die Aufgabe, diese Anforderungen bzw. Vorgaben zu kennen sowie deren Aktualität und Erfüllung (Konformität {Compliance}) sicherzustellen.

Gesetzliche Vorgaben ergeben sich beispielsweise aus dem Bürgerlichen Gesetzbuch (BGB), dem Handelsgesetzbuch (HGB), dem Aktiengesetz (AktG), dem Bundesdatenschutzgesetz (BDSG) und dem Urheberrechtsgesetz (UrhG). Abgeleitete Anforderungen finden sich u. a. in der Abgabenordnung (AO), den verschiedenen Grundsätzen im Kontext ordnungsmäßiger Buchführung, wie GoB, GoBS, GDPdU und GoDV sowie den Anforderungen der Wirtschaftsprüfer in FAIT 1, FAIT 2 und FAIT 3.

Anforderungen an das IT-Sicherheitsmanagement sind in der Normenreihe ISO/IEC 27000 dargelegt, die sich im Aufbau befindet, sowie in den Normen ISO/IEC 17799 und ISO/IEC 13335. Das ITIL® Security und Continuity Management beschreibt Best Practices. Weitere Anforderungen enthält das IT-Grundschutzhandbuch des deutschen BSI mit seinen umfangreichen Grundschutzkatalogen.

Checkliste mit Kontrollen (Controls) zum Konformitätsmanagement	Zwingend/ Optional	Ja (✓) / Nein (-)
Verfügt das Unternehmen über ein <u>Konformitätsmanagement</u> ?	Z	
Sind die relevanten <u>Gesetze, Vorschriften, Ausführungsbestimmungen, Prüfungsrichtlinien, Normen und Standards</u> bzw. die relevanten <u>Passagen</u> daraus sowie <u>vertragliche Verpflichtungen</u> identifiziert, dokumentiert und aktuell?	Z	
Stellt das Konformitätsmanagement sicher, dass es über <u>konformitätsrelevante Entwicklungen</u> so frühzeitig informiert ist, dass es die Konsequenzen bewältigen und effizient in das Unternehmen integrieren kann.	O	
Stellt das Konformitätsmanagement die jederzeitige zeitnahe <u>Information aller Verantwortlichen</u> über die sie betreffenden Konformitätsanforderungen sicher?	Z	
Besitzt das Konformitätsmanagement einen <u>Überblick</u> über die im Unternehmen <u>ergriffenen prozessualen, ressourcenspezifischen und organisatorischen Elemente</u> , welche die Konformitätsanforderungen erfüllen sollen?	Z	
Führt das Konformitätsmanagement selbst oder durch Dritte eine angemessene <u>Verifikation</u> durch, dass die ergriffenen prozessualen, ressourcenspezifischen und organisatorischen Elemente die Anforderungen erfüllen?	Z	
Besitzt das Konformitätsmanagement einen <u>Prüfungsplan</u> (Auditplan)?	Z	
Stellt das Konformitätsmanagement sicher, dass <u>Auditwerkzeuge</u> weder den Betrieb von Systemen stören noch missbräuchlich nutzbar sind?	Z	
...		

9.5.3 Datenschutzmanagement (Privacy Management)

Zur Vermeidung von Datenschutzverletzungen müssen die gesetzlichen Regelungen eingehalten werden. Diese ergeben sich je nach Anwendungsfall aus dem Bundesdatenschutzgesetz (BDSG), den jeweiligen Landesdatenschutzgesetzen (LDSG), dem Teledienstedatenschutzgesetz (TDDSG), dem Telemediengesetz (TMG), dem Sozialgesetzbuch (SGB) etc.

Wesentliche Anforderungen des BDSG, Stand 22. August 2006, spiegeln sich gemäß der dortigen Anlage zu §9 in den folgenden Kontrollen wider:

1. Zutrittskontrolle:
„Maßnahmen [...], die [...] geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren“
2. Zugangskontrolle
„Maßnahmen [...], die [...] geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
3. Zugriffskontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können [...]“
4. Weitergabekontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist“
5. Eingabekontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind“
6. Auftragskontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können“
7. Verfügbarkeitskontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind“
8. Trennungskontrolle
„Maßnahmen [...], die [...] geeignet sind, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“

Checkliste mit Kontrollen (Controls) zum Datenschutzmanagement	Zwingend/ Optional	Ja (✓) / Nein (-)
Verfügt das Unternehmen über ein <u>Datenschutzmanagement</u> ?	Z	
Verfügt das Unternehmen im Hinblick auf datenschutzrelevante Datenverarbeitung über die folgenden <u>Kontrollen</u> : - Zutrittskontrolle - Zugangskontrolle - Zugriffskontrolle - Weitergabekontrolle - Eingabekontrolle - Auftragskontrolle (bei Verarbeitung im Auftrag) - Verfügbarkeitskontrolle - Trennungskontrolle	Z	

9.5.4 Risikomanagement (Risk Management)

Anforderungen

Das Thema Risikomanagement gewinnt zunehmend an Bedeutung, in Deutschland zum einen aufgrund des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), dessen Anforderungen in das Aktiengesetz (AktG) und das Handelsgesetzbuch (HGB) eingeflossen sind. Zum anderen durch Basel II und bei Banken zusätzlich durch die Mindestanforderungen an das Risikomanagement (MaRisk).

Dementsprechend wurde und wird in Unternehmen der Prozess des Risikomanagements etabliert. Hierbei ist teilweise zu beobachten, dass das Risikomanagement, das Sicherheitsmanagement und das Kontinuitätsmanagement als separate Disziplinen angesehen und als solche organisatorisch abgebildet sind. Hier gilt es zu beachten, dass das Sicherheits-, Kontinuitäts- und Risikomanagement Hand in Hand gehen müssen. Warum?

Drei-dimensionale Risiko-management-pyramide nach Dr.-Ing. Müller

Das Risikomanagement geht – wie auch das Sicherheits- und Kontinuitätsmanagement – von der Sicherheits-, Kontinuitäts- und Risikopolitik aus. Es baut auf dem Risikodreiklang auf, d. h. es betrachtet das Bedrohungspotenzial sowie das Schadens- und Schwachstellenpotenzial. Es stellt damit die komplementäre Sichtweise zum Sicherheits- und Kontinuitätsmanagement dar. Ein autarkes Risikomanagement – basierend auf dem allgemeinen dreidimensionalen Pyramidenmodell des Autors – lässt sich analog zur dreidimensionalen Sicherheitspyramide über die dreidimensionale Risiko- bzw. Risikomanagementpyramide nach Dr.-Ing. Müller aufbauen. Hierbei sind die hierarchische Dimension, die Dimension der Prozesse, Ressour-

cen und Organisation für das Risikomanagement (PRORim) sowie die Dimension der Lebenszyklen zu berücksichtigen. Es stehen also auch hier die gleichen Themenfelder an, wie beim Sicherheits- und Kontinuitätsmanagement, nur aus einem anderen Blickwinkel.

Analog zum später beschriebenen Sicherheitsregelkreis erfolgt der Aufbau des Risikoregelkreises. Der Risikomanagementprozess nutzt den Deming- bzw. PDCA-Zyklus, der aus dem Qualitätsmanagement bekannt ist [29]. PDCA steht für die vier Phasen Plan-Do-Check-Act. Der Risikomanagementprozess beinhaltet Steuerung, Monitoring, Controlling und Reporting der Risiken (Soll-Ist-Vergleich) sowie die Risikokommunikation zur frühzeitigen und gezielten Einbindung möglicher Betroffener und Beteiligter. Hierbei sind – wie üblich – alle Elemente des Risikomanagements hinreichend und nachvollziehbar zu dokumentieren. Dies kann beispielsweise über ein intranetbasiertes Risikomanagementhandbuch erfolgen, das über ein berechtigungsgesteuertes Portal erreichbar ist.

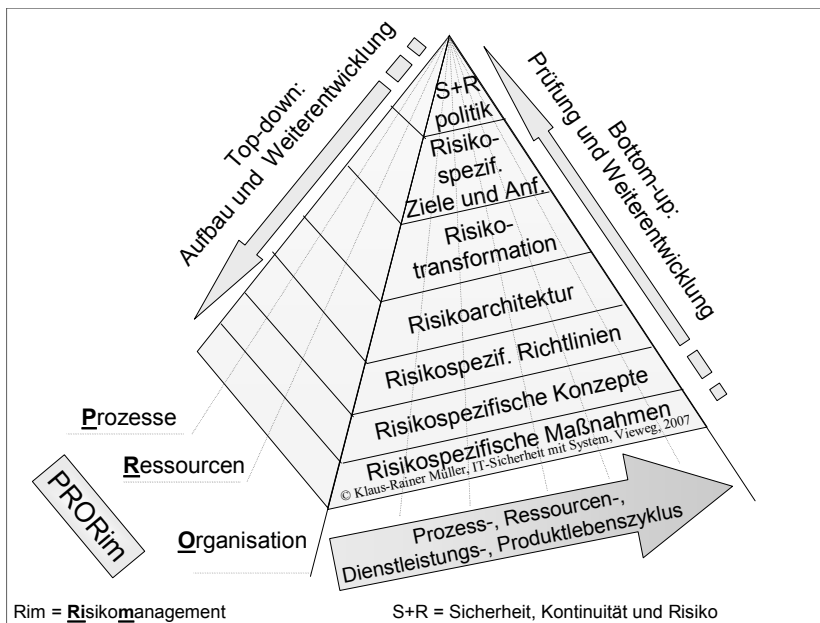


Abb. 9.5: Risikomanagementpyramide nach Dr.-Ing. Müller

Für den hierarchischen Aufbau des Risikomanagements ergeben sich folgende Schritte:

1. Definition der Risikopolitik und –strategie
2. Ermittlung der risikospezifischen Ziele und Anforderungen (s. a. Sicherheitsziele/-anforderungen) der Prozesse und Ressourcen, z. B. niedriges Risiko (= hohe Sicherheit), und darauf aufbauend Bildung von Risikokategorien und Schadenspotenzialklassen durch
 - Schadensanalyse zur Ermittlung des Schadenspotenzials bzw. der Schadenspotenzialklasse der Schutzobjekte (Werte) je Sicherheitskriterium, jedoch noch ohne Berücksichtigung einzelner konkreter Bedrohungen. Es ergibt sich die Schadensarchitektur bzw. Geschäfts- und Ressourceneinflussarchitektur (business/resource impact architecture).

Nach der Schadensanalyse kann der Risikomanager – ähnlich wie auch beim Sicherheitsmanagement nach der Schutzbedarfsanalyse der Sicherheitsmanager – entscheiden, wie kritisch oder auch unkritisch der Prozess oder die Ressource ist. Auf dieser Basis kann er das weitere Vorgehen priorisieren.

3. Transformation der risikospezifischen Ziele und Anforderungen der Kernprozesse auf die Unterstützungs- und Begleitprozesse sowie Ressourcen, Organisation, Produkte und Dienstleistungen. Die Transformation berücksichtigt die Wichtigkeit der jeweiligen Anforderung sowie gegebenenfalls den Schutz vor konkreten Bedrohungen.
4. Entwicklung der Risikoarchitektur bestehend aus prinzipiellen Anforderungen an die maximal tolerierbare Höhe des Risikos, d. h. des Schadensausmaßes bzw. –potenzials, der prinzipiellen Bedrohungen und Schwachstellen sowie der Risikominderungselemente durch
 - Verifizierung und gegebenenfalls Konsolidierung der Schadenspotenzialklassen
 - Verifizierung und gegebenenfalls Konsolidierung der Risikokategorien
 - Bedrohungsanalyse zur Ermittlung des prinzipiellen Bedrohungspotenzials anhand der Bedrohungen und ihrer Eintrittswahrscheinlichkeit sowie zur Erstellung der Bedrohungsarchitektur. Für die Bedrohungsanalyse je Schutzobjekt findet sich mancherorts der Begriff Risikoidentifikation
 - ➔ *Die Kombination aus Schadens- und Bedrohungspotenzial stellt das Brutto-Risikoinventar dar. Die Kombination aus Schadens- und Bedrohungsarchitektur dementsprechend die Brutto-Risikoarchitektur.*

- Schwachstellenanalyse zur Ermittlung des Schwachstellenpotenzials anhand der Schwachstellen und ihrer Wichtigkeit sowie der Schwachstellenarchitektur
 - ➔ *Die Kombination aus Schadens-, Bedrohungs- und Schwachstellenpotenzial stellt das Netto-Risikoinventar dar. Die Kombination aus Schadens-, Bedrohungs- und Schwachstellenarchitektur dementsprechend die Netto-Risikoarchitektur. Die Ermittlung des Risikoinventars durch die Schadens-, Bedrohungs- und Schwachstellenanalyse kann auch als Netto-Risikoinventur bezeichnet werden.*
 - Risikoaggregation, Risikokonzentration und Risikodiversifikation (Risikostreuung)
 - Auswahl risikomindernder Strategien, Prinzipien und Elemente (s. a. Sicherheitsstrategien, -prinzipien und -elemente) sowie Entwicklung der Risiko- und Risikominderungs- bzw. Sicherheitsarchitektur
 - Festlegung von Kontrollen zum Monitoring und Controlling zwecks Aufbau der Kontrollarchitektur, die später in einem Risikoregelkreis (s. a. Sicherheitsregelkreis) Anwendung findet, der sich an der Balanced Scorecard [11] orientieren kann
5. Entwicklung risikospezifischer sowie risikomindernder Richtlinien (Sicherheitsrichtlinien)
 6. Spezifikation risikospezifischer sowie risikomindernder Konzepte (Sicherheitskonzepte)
 7. Umsetzung risikospezifischer sowie risikomindernder Maßnahmen (Sicherheitsmaßnahmen) sowie Allokation von Risikokapital zur Absicherung verbleibender Risiken

Hieraus ist ersichtlich, dass sich in wesentlichen Bereichen direkte inhaltliche Überlappungen zwischen der Risiko- der Sicherheitspyramide des Autors ergeben. Daher empfiehlt es sich, den zuvor geforderten integrativen Ansatz zu verfolgen. Bei Interesse findet sich eine etwas detailliertere Beschreibung der Risikopyramide im „Handbuch Unternehmenssicherheit“.

Einen Überblick über die Risikosituation verschafft die Bruttoreisikomatrix, die im Folgenden prinzipiell, auszugsweise und beispielhaft dargestellt ist. Sie basiert auf einer standardisierten Bedrohungslandkarte mit einheitlichen Eintrittswahrscheinlichkeiten für die betrachteten Schutzobjekte.

Bruttorisikomatrix									
Objekt	Bedrohungen	<- Schadenswert	Wassereinbruch	Feuer	Einbruch	:	:	:	:
Eintrittswahrscheinlichkeit ->			N	N	M	...	...	...	...
IT-System 1		H	M	M	H	...	...	...	...
IT-System 2		N	N	N	N	...	...	...	...
...		...	...	...	...	...	...	...	...

9.5.5 Leistungsmanagement (Service Level Management)

Das Leistungsmanagement (Service Level Management {SLM}) umfasst den Service-Katalog (Service Catalogue) und die Leistungsvereinbarungen (Service Level Agreements {SLA}) mit den externen Kunden. Hieraus leiten sich die Vereinbarungen mit internen Dienstleistern (Operational Level Agreements {OLA}) und externen Dienstleistern (Underpinning Contracts {UC}) ab. Ebenfalls zum SLM gehören die erforderlichen Absicherungen der Dienstleistungen sowie die Überwachung und Steuerung der Leistungserbringung. Die Überwachung und Steuerung der externen Leistungserbringer durch den Auftraggeber ist ein wichtiger Prozess, der kompetentes internes Personal erfordert. Er wird als Provider-Management bezeichnet.

*Kundenanforderungen,
Leistungsspektrum*

Das Leistungsmanagement beginnt mit der proaktiven Ermittlung der kurz-, mittel- und langfristigen Kundenanforderungen (Service Level Requirements {SLR}) durch die Service Manager. Diesen Anforderungen steht das eigene Leistungsspektrum gegenüber, das gegebenenfalls weiterentwickelt wird. Die Service Manager verhandeln mit den Kunden Verträge, stimmen sie intern ab und schließen sie ab bzw. bereiten den Abschluss vor.

Sicherheitsanforderungen

Im Rahmen der Leistungsvereinbarungen müssen die Anforderungen der Kunden konkretisiert und messbar gestaltet werden. Hierzu gehört beispielsweise die Erhebung des Schutzbedarfs bzw. der Sicherheitsanforderungen in Form einer Geschäftseinflussanalyse, des Mengengerüsts mit seiner prognostizierten Entwicklung und Archivierungsanforderungen. Besonderes Augenmerk sollte darüber hinaus auf die Erfassung zu erfüllender Anforderungen des Gesetzge-

bers, von Aufsichtsbehörden und Normierungsgremien gelegt werden, die der Kunde eventuell implizit erwartet.

Aus den Anforderungen der Kunden leiten die Service Manager die eigenen Leistungsangebote ab. Diese können grundsätzlich sowohl intern erbracht als auch extern eingekauft werden. Was ist hierbei zu beachten?

9.5.5.1 Prozessauslagerung (Business Process Outsourcing)

Aufgrund des zunehmenden Wettbewerbs und Kostendrucks, aber auch der Unzufriedenheit mit internen Dienstleistungen lagern Unternehmen Prozesse im Rahmen des Business Process Outsourcing (BPO) ganz oder teilweise aus, beispielsweise den Objektschutz, Sicherheitsdienste, Gehaltsabrechnungen, Call-Center, User Help Desks, PC Services, Web Hosting und den Betrieb von Rechenzentren und Anwendungen. Im Bankenbereich sind so Transaktionsbanken und Kreditfabriken entstanden. Versicherungen nutzen Call Center und Application Service Provider für Bestandsführungssysteme.

*Prozess-
auslagerung*

Den Chancen des Outsourcing stehen jedoch auch vielerlei Risiken bei Kosten, Leistung, Qualität und Sicherheit gegenüber. Aus gutem Grund fordert die BaFin in ihrem Rundschreiben 11/2001 [30], die „Auslagerungsunternehmen mit der erforderlichen Sorgfalt auszuwählen“ und „die Leistungserbringung [...] laufend zu überwachen“. Dem Outsourcing aufgrund von Adhoc-Entscheidungen zum Sparen und Flexibilisieren von Kosten oder zur Qualitätsverbesserung stehen so manches Mal übersehene Zusatzkosten für die Steuerung der Outsourcing-Unternehmen oder auch verlorene Kernkompetenzen gegenüber.

*Chancen und
Risiken des
Outsourcing*

Doch trotz vermeintlich sorgfältiger Auswahl und Vorbereitung kommt es verschiedentlich zu Schwierigkeiten, vor allem in der Übergangsphase und im Betrieb. Die Folge sind Performance-Engpässe, Störungen und in ungünstigen Fällen Betriebsunterbrechungen. Die Reputation und Handlungsfähigkeit, gegebenenfalls sogar die Existenz des Unternehmens stehen auf dem Spiel. Was ist zu tun?

Risiken sollten durch eine systematische Vorgehensweise auf ein vertretbares Maß reduziert werden. Die Entscheidung für „make or buy“ sollte professionell getroffen werden, z. B. anhand der dreidimensionalen Sourcing-Pyramide nach Dr.-Ing. Müller. Sie bietet ein wegweisendes und praxisorientiertes Vorgehensmodell und basiert auf dem allgemeinen Pyramidenmodell des Autors. In ihrer kompakten Form wurde sie im Sommer 2004 publiziert [31]. In ausführliche-

*Dreidimen-
sionale
Sourcing-
Pyramide nach
Dr.-Ing. Müller*

	rer Form einschließlich der Richtlinie Sourcing findet sie sich im „Handbuch Unternehmenssicherheit“ des Autors.
<i>Sourcing-Ziele und -Anforderungen</i>	Seine Sourcing-Ziele und -Anforderungen sollte das Unternehmen klar und unter Berücksichtigung aller erforderlichen Sicherheitskriterien und -aspekte formulieren. Geeignete Rahmenwerke zu Service-Vereinbarungen stellen sicher, dass formale, juristische, prozessuale, ressourcenspezifische und organisatorische Aspekte angemessen berücksichtigt und über Kennzahlen nachgewiesen werden.
<i>Auditierung, Prüfung und Bewertung</i>	Richtlinien zur Auditierung, Prüfung und Bewertung potenzieller Dienstleister im Vorfeld der Auftragsvergabe beziehen sich auf deren Leistungsfähigkeit, Qualität, Sicherheit, Referenzen und Marktstärke. Die Eigentümerstruktur sollte im Hinblick auf mögliche Interessenkonflikte durchleuchtet werden. Risiken, wie z. B. die Insolvenz eines Dienstleisters, sind zu bewerten und gegebenenfalls abzusichern. Bei der Prüfung vor Ort und der Entwicklung der Checkliste zu sicherheitsrelevanten Aspekten empfiehlt sich der Einsatz erfahrener externer Berater.
<i>Provider-Management: Überwachung und Steuerung in der Praxis</i>	Die Überwachung und Steuerung des oder der Auslagerungsunternehmen benötigt erfahrene eigene Mitarbeiter. Der Aufbau eines Provider-Managements mit Prozessen, Ressourcen und geeigneter Organisation ist erforderlich. Darüber hinaus müssen die Service-Vereinbarungen messbar sein. Service-Manager müssen durch vertragliche Vereinbarungen in die Lage versetzt sein, die Leistungserbringung durch ein kontinuierliches Monitoring verfolgen zu können. Diese Aspekte sind bei der Bewertung der Wirtschaftlichkeit, Qualität und Strategiekonformität von Outsourcing-Projekten sowie der SLA-Gestaltung wesentlich.
<i>Tücken des Multi-Provider-Managements</i>	Insbesondere der Einsatz mehrerer Provider erhöht die Komplexität der Steuerung und des Zusammenspiels der Provider, die vom Multi-Provider-Management des auslagernden Unternehmens zu leisten ist. Betrachten wir ein – im Vergleich zu mancher von mir erlebten Konstellation – „einfaches“ Beispiel: das auslagernde Unternehmen hat Verträge mit drei Providern. Es greift über das Weitverkehrsnetz des Providers 1 auf die Anwendungen des Providers 2 zu, die vom Provider 3 gehostet werden. Plötzlich sind keine Eingaben mehr möglich. Es stellt sich die Frage: wo liegt der Fehler? Im eigenen LAN, im WAN, in der Anwendung oder ist der Host ausgefallen? Je nach Provider und dessen Professionalität erhalten Sie hierzu entweder sofort die entsprechende Benachrichtigung und Information oder Sie erfahren von Ihren Providern, dass alles in Ordnung ist. Dann müssen Sie sich selbst auf die manchmal aufwändige Suche

nach der Fehlerursache machen. Hilfe leisten Ihnen dabei ein übergreifendes Monitoring mit aktuellen und korrekten Daten all Ihrer Provider sowie idealerweise zusätzliche providerübergreifende SLAs. In diesen verpflichten sich die Provider zur Kommunikation und Kooperation mit den anderen beteiligten Providern sowie zur Erfüllung der Service- und Performance-Anforderungen der anderen Provider.

Unabhängig von den Entscheidung für „make or buy“ gilt es, den Überblick zu wahren über die Verträge mit Kunden, internen Bereichen und externen Dienstleistern. Was ist hier zu beachten?

9.5.5.2 Vertragsmanagement

Die Verträge mit den Kunden finden ihren Niederschlag in Vereinbarungen mit internen Abteilungen (Operational Level Agreements {OLA}) und Verträgen mit den dazu erforderlichen Dienstleistern (Underpinning Contracts {UC}).

Dienstleister

Bevor Unternehmen diese Verträge abschließen, sollten sie die Dienstleister z. B. im Hinblick auf ihre Leistungsfähigkeit, Qualität, Sicherheit, Referenzen und Marktstärke prüfen. Hierbei sollten sie Risiken, wie z. B. die Insolvenz eines Dienstleisters, bewerten und gegebenenfalls abgesichern.

Service-Manager überwachen anschließend kontinuierlich die Erfüllung der Verträge und dokumentieren sie in Berichten. Die Überwachungsergebnisse lassen sich zur Verbesserung der Leistungen und gegebenenfalls Veränderung des Leistungsangebots sowie der Verträge nutzen. Ferner führen die Service-Manager auf dieser Basis Lieferantenbewertungen durch.

*Leistungs-
verfolgung*

Quellcode in neutraler Hand

Die Vergabe von Software-Entwicklungsaufträgen – sei es zur Neuentwicklung, Weiterentwicklung oder Anpassung – aber auch die Lizenznahme birgt Risiken. Eins dieser Risiken ist die Insolvenz des Auftragnehmers, dessen Brisanz mit steigendem Auftragswert und Lizenzvolumen zunimmt. Dementsprechend sollte ein Unternehmen dieses Risiko in Abhängigkeit von der Kritikalität der Anwendungen und der relevanten finanziellen Schmerzgrenze, z. B. ab 0,5 Mio. EUR, angemessen absichern.

Eine Möglichkeit besteht darin, den Quellcode bei einem Notar für den Fall der Insolvenz des Auftragnehmers hinterlegen zu lassen. Eine andere ist die Beauftragung einer so genannten Escrow-Agentur, die den Quellcode als Zwischeninstanz treuhänderisch bis zu einem vordefinierten Ereignis, der Insolvenz, verwaltet. Escrow-Agenturen bieten u. a. an, zu prüfen, ob die gelieferten Datenträger lesbar und virenfrei sind sowie den Quellcode



*Escrow-
Agentur*

enthalten. Die Dienstleistungen können bis hin zum Kompilieren und Testen sowie die Einbindung in das Update-Verfahren gehen.

Auch hier gilt – wie bei allen Dienstleistern – dass der Auftraggeber den Treuhänder im Vorfeld bewerten sollte.

Verträge mit Dienstleistern

Verträge mit internen und externen Dienstleistern können in jeder Phase des Lebenszyklus von ITK-Systemen erforderlich sein. Die Vertragspartner können vielfältiger Natur sein, vom externen Berater oder Programmierer über System- und Software-Häuser, Lizenzgeber, den Third Level Support, Outsourcing- und Versorgungsunternehmen sowie Vermieter bis hin zum Versicherungsunternehmen, das z. B. Betriebsunterbrechungen versichert.

Managed Services

In letzter Zeit kommen Anbieter von Managed Services hinzu. Hierzu gehören Service Provider für Application, Internet, Storage, VPN oder auch Security.



Vertragsdatenbank

Vertragsdatenbank

Um den Überblick über die Verträge mit internen und externen Kunden und Dienstleistern zu behalten, empfehle ich auslagernden Unternehmen – wenn wirtschaftlich sinnvoll – eine Vertragsdatenbank (SLA-, OLA-, UC-Datenbank) zu führen. Diese sollte auch Versicherungs- und Lizenzverträge umfassen. Die Vertragsdatenbank nimmt alle relevanten Vertragsdaten auf, wie z. B. Vertragsidentifikator, Vertragsgegenstand, Vertragsart (z. B. Dienstleistung, Gewerk; Aufwand, Festpreis; Entwicklung, Betrieb, Wartung, etc.), Vertragspartner, Ansprechpartner und deren Erreichbarkeit, Start- und Endedatum des Vertrags, Kennzahlen des Vertrags (z. B. zu Reaktionszeiten, Service-Zeiten), Verweis auf den Originalvertrag und dessen Aufbewahrungsort sowie Bemerkungen.

9.5.6 Finanzmanagement (Financial Management)

Die verfügbaren finanziellen Mittel spielen im Lebenszyklus von ITK-Systemen eine wesentliche Rolle. Leistungserfassung, Leistungsnachweis, Leistungsabrechnung und Controlling sind wesentliche Aktivitäten im Finanzmanagement. Unternehmen müssen geplante Investitionen im Vorfeld über den ganzen Lebenszyklus und unter Berücksichtigung von Sicherheitsaspekten betrachten, um Fehlentscheidungen zu vermeiden.



Unnötige Mehrkosten

Eine Fachabteilung eines Unternehmens beantragte ein neues Informationssystem. Im Projektantrag berücksichtigte sie nur die Hardware- und Entwicklungskosten, nicht jedoch die späteren Betriebskosten. Deren Be-

rücksichtigung hätte anstelle einer Vielzahl in der Anschaffung günstiger kleinerer Server zur Auswahl eines größeren, leichter abzusichernden und zu betreuenden Rechners geführt.

9.5.7 Projektmanagement (Project Management)

**Planung schafft Sicherheit,
Planlosigkeit birgt Risiken.**

Nur Genies beherrschen das planlose Chaos – manchmal.

(© Klaus-Rainer Müller, 3. Februar 2007)



Damit die Sicherheitsthematik im Lebenszyklus eines Informationssystems von Anfang an berücksichtigt wird, muss sie im Lebenszyklus von Informationssystemen verankert sein. In den Anfangsphasen des Lebenszyklus bis zur Inbetriebnahme werden Informationssysteme in der Regel als Projekte durchgeführt. Demzufolge muss in den Projektmanagement-Standards festgelegt oder referenziert sein, am Ende welcher Entwicklungsphase welche sicherheitsrelevanten Ergebnisse in welcher Form geliefert werden müssen. Beispielsweise erfolgt im Rahmen der fachlichen Spezifikation eine Schutzbedarfsanalyse.

9.5.8 Qualitätsmanagement (Quality Management)

Das Qualitätsmanagement begleitet alle Phasen des Lebenszyklus eines Informationssystems. Dementsprechend legen der Sicherheits- und der Qualitätsmanager fest, wie die geforderte Qualität auch der sicherheitsrelevanten Ergebnisse erreicht und geprüft wird. Für die Schutzbedarfsanalyse entwickelt der Sicherheitsmanager beispielsweise eine standardisierte Vorlage, sodass die erforderliche Vollständigkeit erreicht werden kann. In einem Review prüft der Sicherheitsmanager die Inhalte auf die geforderte Vollständigkeit, Korrektheit und Plausibilität. Außerdem verifiziert er sie unter Kosten-Nutzen-Aspekten.

Das Testmanagement kann entweder als Teil des Qualitätsmanagements angesehen werden oder als separater Prozess definiert werden. Wesentlich ist, dass in ihm Tests vorgesehen sind, welche die Einhaltung der Sicherheitsanforderungen und des geforderten Sicherheitsniveaus überprüfen. Dies erfordert beispielsweise Last-, Performance-, Ausfall-, Ende-zu-Ende- (E2E) und Angriffstests. Bei der Lieferung ausführbarer Programme und des Quellcodes sollte der Empfänger über einen Generierungslauf sicherstellen, dass das ausführbare Programm auf dem gelieferten Quellcode basiert.

*Test-
management*

9.5.9 Ereignismanagement (Incident Management)

Im laufenden Betrieb der ITK treten in der Regel immer wieder Fragen, Schwierigkeiten, Störungen und Probleme auf. Um Beeinträchtigungen des Geschäftsbetriebs zu minimieren und die Geschäftskontinuität aufrecht zu erhalten, muss der Umgang mit derartigen Ereignissen definiert sein. Ziel ist es, das jeweilige Ereignis kurzfristig einer Lösung zuzuführen und sei es auch nur durch einen Restart oder in Form einer Umgehung (Workaround). Es geht also um Schnelligkeit und nicht um Ursachenforschung und -behebung. Hiermit beschäftigt sich das Ereignismanagement.

Die neutrale Bezeichnung „Ereignis“ verwende ich deshalb, weil nicht alle gemeldeten „Ereignisse“ tatsächlich eine Störung oder ein Problem darstellen. In der Informationsverarbeitung sitzt das Problem auch manchmal vor dem Bildschirm ☺, allerdings häufig wegen Verletzung des Poka-Yoke-Prinzips durch die ITK.

Aus Gründen der Effizienz und Sicherheit empfiehlt es sich, eine (zentrale) Anlaufstelle („Single Point of Contact“ {SPoC}) bzw. zentrale Ansprechpartner festzulegen. Im Bereich der ITK ist dies oftmals der zentrale Benutzerservice (User Help Desk, Service Desk).

Für Unternehmen, die in den USA börsennotiert sind, ergibt sich ein weiterer Grund für die Einrichtung eines Service Desks. Für sie gilt der Sarbanes-Oxley Act (SOX). Die dortige Section 409 fordert, dass wesentliche Änderungen der finanziellen Situation oder im Geschäftsbetrieb umgehend zu veröffentlichen sind. („Each issuer [...] shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer [...]).“). Da die ITK die Daten für die Quartals- und Jahresberichte verarbeitet, müssen die SOX-relevanten ITK-Systeme und Daten identifiziert sein. Hieraus ableitbar ist, dass Störungen, die das Erkennen wesentlicher Änderungen der finanziellen Situation oder die umgehende Veröffentlichung behindern, vermieden bzw. schnellstmöglich behoben werden müssen. Hier kommt auch der Service Desk ins Spiel, dessen Aufgabe die Minimierung von Beeinträchtigungen des Geschäftsbetriebs ist.

COBIT®, das Wirtschaftsprüfer zur Prüfung der ITK heranziehen, fordert in der Version 4.0 in DS8 (Delivery & Support) einen Service Desk. Der Service Desk fungiert als Verbindung zwischen Benutzer und IT. Seine Aufgabe besteht darin, Anfragen und Störungsmeldungen sowie Service- und Informationsanforderungen entgegenzunehmen, zu registrieren und zu dokumentieren sowie zu kommunizieren und weiterzuleiten. Der Service Desk soll die gemeldeten Er-

eignisse gemäß den vereinbarten Service Leveln klassifizieren und priorisieren sowie verfolgen und gegebenenfalls eskalieren. Ferner fordert COBIT® die Nutzung dort konkret angegebener Kennzahlen.

Die folgende Aufzählung nennt Beispiele von Leistungskennzahlen (Key Performance Indicator {KPI}) für den Service Desk, die dieser messen, analysieren und berichten sollte:

- Zufriedenheit der Benutzer mit dem Service Desk
- Schulungstage pro Mitarbeiter und Jahr
- Anzahl von Anrufen
- Sofortlösungsquote
- Antwortzeiten in Abhängigkeit von der Dringlichkeit
- durchschnittliche Bearbeitungsdauer von Störungen in Abhängigkeit von ihrem Schweregrad bzw. ihrer Dringlichkeit
- durchschnittliche Anzahl bearbeiteter Anrufe pro Mitarbeiter und Stunde
- Anzahl sicherheitsrelevanter Anfragen
- Anzahl kontinuierlich relevanter Anfragen
- Anzahl offener Anfragen insgesamt und je Kategorie
- Anzahl nach Abschluss erneut geöffneter Anfragen
- Anzahl wiederkehrender Anfragen
- Einhaltung der Service Level.

Zum Zwecke der kontinuierlichen Verbesserung kann der Service Desk diese Informationen unter Berücksichtigung von Kosten-Nutzen-Aspekten im Hinblick auf folgende Punkte auswerten und berichten:

- ihre Verläufe pro Tag, Monat und Jahr sowie im Vergleich zu Vorjahren
- ihr Typ, wie z. B. Passwortrücksetzung
- ihre Korrelation zu den zugrunde liegenden Ereignissen, wie z. B. Releasewechsel, Konfigurationsänderung oder Roll-out einer neuen Anwendung
- ihr Bezug zu den jeweiligen Konfigurationselementen, wie Druckern oder Anwendungen, sowie
- Trends.

Der Service Desk stellt den 1st level support dar. Er löst Störungen entweder selbst oder koordiniert die Störungsbehebung. Seine Aufgabe besteht dabei darin, den regulären Betrieb im Rahmen der vereinbarten Service Level und konform mit den Geschäftsanforderun-

gen wiederherzustellen. Je nach unternehmensspezifischer Aufgabenstellung bearbeitet bzw. koordiniert er darüber hinaus Leistungsanforderungen (service requests), wie den Toner-Wechsel, die Behebung eines Papierstaus im Drucker oder das Zurückspeichern (restore) von Daten bis hin zur Beschaffung eines PCs oder Druckers u.ä.

Der 2nd level support mit seinen Spezialisten, z. B. für Datenbanken oder Netz, unterstützt ihn in schwierigeren Fällen. Der 3rd level support schließlich ist meist beim Hersteller oder der internen Entwicklungsabteilung angesiedelt.

*Prozess
Ereignis-
management*

Der Prozess Ereignismanagement beschreibt den Umgang mit den genannten Ereignissen. Der Ablauf enthält die Entgegennahme einschließlich Kategorisierung und Klassifizierung der Ereignisse, deren anschließende Bearbeitung, die Verfolgung und gegebenenfalls Eskalation sowie die Erfassung des Bearbeitungsaufwands. Ebenfalls genannt werden die im Prozess genutzten Hilfsmittel und Werkzeuge. Welche sind dies?

*Hilfsmittel und
Tools*

Zu den Hilfsmitteln gehören beispielsweise Definitionen von Ereignisklassen und -kategorien. Als Tools kommen üblicherweise die Konfigurationsdatenbank und ein „Trouble-Ticket-Tool“ zum Einsatz. Die Konfigurationsdatenbank aus dem Prozess Konfigurationsmanagement dient als Informationsquelle. Im „Trouble-Ticket-Tool“ erfassen die Service-Desk-Mitarbeiter die Ereignisse und dokumentieren die Bearbeitungsschritte und den Bearbeitungsstatus. Das Tool verfolgt den Status und eskaliert gegebenenfalls nach vorgegebenen Regeln. Dadurch, dass die Beteiligten die Bearbeitung der Störungsbehebung im Tool beschreiben, lässt es sich bei geeigneter Funktionalität später als Wissensbasis nutzen. Bei wiederkehrenden oder vergleichbaren Ereignissen greifen die Service-Desk-Mitarbeiter hierauf zurück und können so die Bearbeitungsdauer senken und die Effizienz steigern.

Die Service-Desk-Mitarbeiter sollten darüber hinaus über anstehende und aktuell durchgeführte Änderungen informiert sein, da sich in diesem Zusammenhang leicht Störungen ergeben können. Die Kenntnis dieser Änderungen erleichtert gegebenenfalls die Bearbeitung gemeldeter Ereignisse.

*Kategorisierung
und
Auswertung*

Die Kategorisierung der Ereignisse und deren regelmäßige Auswertung ermöglichen Trendanalysen sowie proaktive und effizienz- sowie sicherheits- und kontinuieritätssteigernde Maßnahmen. Übergreifende Kategorien können z. B. Hardware und Software sein. Spezifische Kategorien beziehen sich auf Passwörter, Computer, Anwendungen, Drucker, Dienstleister, etc.

Ein häufig auftretendes Ereignis ist das Vergessen des Passwortes und dessen Rücksetzung durch die Administration. Der hierfür verbrauchte Aufwand kann aufgrund der Auswertung beispielsweise in Relation zu den Kosten für ein Single-Sign-on-System gesetzt werden und gegebenenfalls dessen Anschaffung begründen.

Ähnlich verhält es sich mit technischen Geräten. Häufige Verfügbarkeitseinschränkende Störungen an technischen Geräten, wie z. B. Druckern, PCs, etc. können genutzt werden, um zukünftige Kaufentscheidungen zu beeinflussen oder das Gespräch mit dem Hersteller zu suchen. Wiederkehrende Schwierigkeiten bei der Nutzung einzelner Informationssystemen können zu einer Weiterentwicklung der Anwendung oder zu verbesserten Schulungsangeboten genutzt werden.

Die Klassifizierung eines Ereignisses dient dessen Priorisierung und bestimmt die Vorgehensweise und die zugesicherte Behebungsdauer. Die genauest mögliche Klassifizierung ist unter Sicherheitsaspekten unumgänglich, um schnelle und zielgerichtete Maßnahmen einzuleiten. Hierbei ist der Zugriff auf die Konfigurationsdatenbank auch deshalb entscheidend, um die Sicherheitsklasse der betroffenen Ressource, die dazugehörigen SLAs sowie die abhängigen Ressourcen und Prozesse ermitteln und die Auswirkungen abschätzen zu können.

Klassifizierung

Der Service Desk ist erste Anlaufstelle für die Meldung sicherheits- und kontinuierkeitsrelevanter Störungen. Damit er solche Ereignisse erkennen kann (Security/Continuity Incident Detection), sollten diese spezifiziert sein. Zu sicherheitsrelevanten Ereignissen gehören beispielsweise der Verlust oder Diebstahl einer Ressource, wie z. B. eines PCs, eines Notebooks, eines PDAs, eines memory sticks oder einer Chipkarte für den Zugang zu Computersystemen und Anwendungen, aber auch Hackerangriffe sowie der Befall durch Computerviren. Zu kontinuierkeitsrelevanten Ereignissen zählen u. a. der Ausfall unternehmenskritischer Anwendungen oder Computer sowie kritische Netzausfälle, die beispielsweise einen Standort lahm legen.

Vorgehensweise

Je Ereignistyp ist die anschließende Vorgehensweise des Service Desks festzulegen, also die Reaktion bzw. Antwort auf das jeweilige sicherheits- oder kontinuierkeitsrelevante Ereignis (Security/Continuity Incident Response). Hierzu gehört auch die Benennung der zuständigen Abteilung bzw. Rolle, die zu informieren oder hinzuzuziehen ist oder an welche die weitere Bearbeitung zu leiten ist. So kann für einen berechtigten Mitarbeiter aufgrund fehlerhafter IT-technischer Umstellungen z. B. der Zugriff auf Anwendungen oder Daten geblockt sein, für die er zuvor berechtigt war. Der Service Desk leitet die Anfrage an die zuständige Stelle, z. B. den Sicherheitsbeauftrag-

ten oder Ressourcenverantwortlichen, zur Prüfung und Bearbeitung weiter.

Zu kritischen Ereignistypen gehören ferner Eskalationspläne, in denen niedergelegt ist, wer in welcher Reihenfolge zu informieren ist, beispielsweise der UHD-Manager, der Chief Information Security Officer (CISO) und ein eventuelles internes CERT (Computer Emergency Response Team) bzw. CSIRT (Computer Security Incident Response Team). Darüber hinaus sind auf revisionssichere und gerichtsfest nachvollziehbare Weise gegebenenfalls Festplattenimages für spätere forensische Untersuchungen zu erstellen. Bei geschäftskritischen Ausfällen sind beispielsweise Mitarbeiter und externe Dienstleister zu informieren und präventiv in Bereitschaft zu versetzen.

Das Rücksetzen des Passwortes wegen Vergessens ist mit geschätzten ca. 20 % bis 30 % des Call-Aufkommens ein recht häufiges sicherheitsrelevantes Ereignis. Hierbei treten Call-Spitzen insbesondere nach der Urlaubszeit auf. Für das Rücksetzen des Passwortes muss ein Vorgehen definiert sein, das mit dem Sicherheitsbeauftragten und der Revision abgestimmt ist. Zu achten ist hierbei u. a. darauf, dass der Anfordernde zweifelsfrei identifiziert ist, die Übermittlung des Passwortes sicher ist und die Änderung des zurückgesetzten Passwortes innerhalb kurzer Zeit erfolgen muss. Findet die Änderung nicht innerhalb der vorgegebenen Zeitspanne statt, sollte das Benutzerkonto automatisch gesperrt werden.

Im Rahmen des Reporting sollte der Service Desk auf das Call-Volumen und Call-Häufungen eingehen und diese analysieren. Die Analyse bezieht sich hierbei zum einen auf den verursachten Aufwand und die entstandenen Kosten für den Service Desk und zum anderen auf Aufwand, Kosten und entgangenen Gewinn der betroffenen Geschäftsprozesse und Mitarbeiter. Der Bericht des Service Desk sollte aus der Analyse Handlungsempfehlungen ableiten. Hinsichtlich der Passwort-Rücksetzung könnten dies beispielsweise Single-Sign-on-Systeme und Self-Service-Funktionen zur Passwort-Rücksetzung sein.

Damit die Mitarbeiter des Service Desks in der Lage sind, angemessen auf sicherheits- und kontinuierkeitsrelevante Ereignisse zu reagieren, sind Schulungen, kontinuierliche Information über aktuelle und neue Bedrohungen sowie Sensibilisierungsmaßnahmen und themen- und kritikalitätsbezogenen Übungen erforderlich. Außerdem ist die Kenntnis der IT-Architektur sowie der Kritikalität ihrer Komponenten notwendig.

Die Verantwortlichkeit für die interne und externe Kommunikation gravierender Ereignisse ist ebenfalls festzulegen. Hierzu gehört die Angabe, in welcher Reihenfolge wer über welches Medium und in welcher Form zu informieren ist. Außerdem ist festzulegen, ob das sicherheitsrelevante Ereignis vertraulich zu handhaben ist, um negative Außenwirkungen zu begrenzen und/oder eigene Nachforschungen und Gegen- und Abwehrmaßnahmen nicht durch frühzeitige Information des Angreifers zu beeinträchtigen.

Kommunikation

Je nach Unternehmen und Unternehmensgröße unterscheidet sich der Prozess des Ereignismanagements und die unterstützenden Tools. Insbesondere kleinere Unternehmen erfassen gegebenenfalls nur solche Ereignisse, die ein tatsächliches Problem darstellen oder deren Bearbeitung kompliziert und/oder aufwändig ist.

*Ereignis-
management
und
Unternehmens-
größe*

Der Service Desk bzw. das Ereignismanagement stellen, wie viele andere Begleitprozesse auch, Anforderungen an unterstützende Begleitprozesse und Ressourcen bis hin zu externen Dienstleistern. Diese Anforderungen ergeben sich aus den expliziten Service-Vereinbarungen des Service Desks mit seinen Kunden hinsichtlich Servicezeiten und maximal tolerierbaren Ausfallzeiten. Dementsprechend vereinbart der Service Desk Operational Level Agreements (OLAs) mit seinen internen bzw. Underpinning Contracts (UCs) mit seinen externen Servicegebern.

*Operational
Level
Agreements
und
Underpinning
Contracts*

Zu den Vereinbarungen gehören z. B. die Anforderungen, dass Tools, wie das Ticket System, die Configuration Management Database (CMDB), E-Mail und ein gegebenenfalls genutztes CTI-System (Computer-Telephone-Integration) innerhalb der Service-Zeiten des Service Desks im geforderten Umfang verfügbar sein müssen. Entsprechendes gilt für die erforderlichen Ansprechpartner außerhalb des Service Desk. Verbindungen bestehen hierbei z. B. zur Anwendungsbetreuung, zur IT-Infrastruktur, zur IT-Sicherheit, zum IT-Notfallbeauftragten und zu externen Dienstleistern.

Darüber hinaus stellt der Service Desk Anforderungen, die für eine professionelle Abwicklung seiner Aufgaben erforderlich sind. Hierzu gehört die rechtzeitige Information über anstehende Änderungen, aus denen sich potenzielle Störungen des Betriebs ergeben können. Beispiele hierfür sind Hard- oder Software-Änderungen. Dies schließt Patches ein. Ein weiteres Thema ist die frühzeitige Information z. B. durch den Sicherheitsbeauftragten über neue Bedrohungen, deren Auftreten und Auswirkungen sowie die dazugehörige Vorgehensweise seitens des Service Desk.

Kontinuitätsmanagement

Damit aus dem SpoC („Single Point of Contact“), kein SpoF („Single Point of Failure“) wird, behandelt der Service Desk auch für sich selbst das Thema Kontinuitätsmanagement. Hierzu erstellt er Notfallpläne für den Ausfall jener Prozesse und Ressourcen, die er zur Erfüllung seiner Aufgaben benötigt. Beispiele hierfür sind der Ausfall des CTI-Systems oder des Ticket Systems. Als Workaround bietet sich das Arbeiten des Service Desks ohne CTI über eine Sammelrufnummer an sowie die Nutzung einer lokalen vorstrukturierten Datenbank oder eines Tabellenkalkulationsprogramms für die Entgegennahme und Bearbeitung der Calls. Die Service-Desk-Mitarbeiter müssen diese Einträge bei Verfügbarkeit des Ticket Systems dann entsprechend nachpflegen. Diese Nacharbeiten sind einzuplanen.

9.5.10 Problemmanagement (Problem Management)

Probleme treten erfahrungsgemäß im Lebenszyklus eines ITK-Systems immer wieder auf. Sie können in Form von Beeinträchtigungen, Störungen und Fehlern auftreten, beispielsweise in der Testphase oder im Betrieb. Sie zu erfassen, zu untersuchen und einer langfristigen Lösung zuzuführen, ist Aufgabe des Problemmanagements. Das Problemmanagement wird hierbei u. a. gespeist von denjenigen Ereignissen im Ereignismanagement, die ein tatsächliches Problem darstellen.

Prozess und Hilfsmittel

Der Prozess des Problemmanagements beschreibt, wie Fehler erfasst, kategorisiert, klassifiziert, untersucht, behoben, verfolgt (tracking) und eskaliert werden. Problemkategorien sind beispielsweise Hardware, Software und Paperware, die nutzenorientiert jeweils weiter unterteilt werden können, z. B. Hardware in Computer, Speicher, Drucker, Kommunikationseinheiten. Fehlerklassen legen die Gravität von Fehlern sowie die Zeitdauer für die Beantwortung und Behebung fest.

Darüber hinaus muss festgelegt werden, wie die Problemlösung getestet, freigegeben und wieder in Betrieb genommen wird. Fehler und deren Lösung werden zur jederzeitigen Nutzung in einer Datenbank festgehalten. Idealerweise ist diese Teil einer Anwendung, die über ein standardisiertes Berichtswesen und Eskalationsprozeduren verfügt.

Auswertungen

Auswertungen der Probleme geben Auskunft darüber, wann und in welcher Lebenszyklusphase wer welches Problem mit welchem Schweregrad gemeldet hat, wie viele Probleme sich in welchem Status befinden, wie lange die Problembehebung dauerte, wie sich die Probleme auf die Problemkategorien und die einzelnen Konfigurationselemente verteilen, etc. Hieraus ergeben sich Trends und Erkenntnisse, die für die effiziente und zielgerichtete Steuerung der ITK

nützlich sind. Die Auswertungen können beispielsweise zur Bewertung und proaktiven Weiterentwicklung der internen Prozesse, z. B. des Projekt- und Qualitätsmanagements, und der Dienstleister herangezogen werden. Problemhäufungen können zum Wechsel des Dienstleisters bzw. Lieferanten oder der Hardware führen.

Probleme erst im Betrieb

Die Entwicklung von ITK-Systemen ist bekanntermaßen ein komplexer, risikobehafteter und nicht immer erfolgreicher Prozess. Neben einer Vielzahl gescheiterter Projekte gehen aus Termingründen durchaus auch instabile und unzureichend getestete Informationssysteme in Betrieb. Die Auswertung der Problemmeldungen (Problem Records) und die Bewertung der Projektmanager auch anhand der im Betrieb aufgetretenen Probleme lässt sich als weiteres Anreiz- und Steuerungselement im Personalbereich nutzen.



9.5.11 Änderungsmanagement (Change Management)

Probleme oder neue Anforderungen führen zu Änderungsanfragen (Change Request {CR}). Diese können sich u. a. auf Prozesse und Ressourcen, wie z. B. Informationssysteme, sowie auf Produkte und Dienstleistungen beziehen. Änderungsanforderungen enthalten eine Begründung, Angaben zu den betroffenen Ressourcen (Konfigurationselemente) sowie gegebenenfalls den Bezug zu Problemen, die durch die Änderung gelöst werden sollen. Die Bearbeitung, Genehmigung oder Ablehnung von Änderungsanfragen erfolgt nach einem unternehmensspezifisch definierten Verfahren des Änderungsmanagements.

*Änderungs-
anfragen
(Change
Requests)*

Das Änderungsmanagement (Change Management) erfasst die anliegenden Änderungsanforderungen, kategorisiert sie nach Schutzobjektklasse, priorisiert sie nach Dringlichkeit und klassifiziert sie nach den potenziellen Auswirkungen. Hierbei berücksichtigt es die Service Level Agreements und die maximal tolerierbaren Ausfallzeiten.

*Änderungs-
management
(Change
Management)*

Die Auswirkungen der beantragten Änderungen sowie deren Interdependenzen werden analysiert, um anschließend vom Änderungsmanager selbst – oder bei risikoreichen Änderungen von einem Gremium – abgelehnt oder genehmigt, priorisiert und geeignet terminiert zu werden. Das Änderungsgremium umfasst neben dem Änderungsmanager kompetente Vertreter der Nutzer und des IT-Betriebs, den Architekturmanager sowie den Sicherheitsmanager. Änderungspläne halten die geplante Reihenfolge der durchzuführenden Änderungen fest.

Der Änderungsmanager beauftragt anschließend die genehmigten Änderungen und entwickelt in Abhängigkeit von deren potenziellen Auswirkungen Rückfallpläne. Nach Realisierung, Test und erfolgreicher Abnahme gibt er die Änderungen frei. Eine Änderungshistorie (Change History) hält die durchgeführten Änderungen nachvollziehbar fest.

*Geordneter
Änderungs-
prozess*

Das Änderungsmanagement schafft somit einen geordneten Änderungsprozess, der das Risiko von Fehlern oder Ausfällen aufgrund von Änderungen proaktiv verringern hilft. Eine Verbindung zum Ereignismanagement ist wesentlich, damit dort Informationen über aktuelle oder anstehende Änderungen bei der Bearbeitung von Ereignissen und Störungen genutzt werden können.



Phänomen der „alten“ Fehler

Nutzer stellen hin und wieder fest, dass bereits behobene Fehler in einem neuen Release unerklärlicherweise wieder auftauchen. Eine Ursache liegt in einem unzureichenden Änderungsverfahren. Während ein Entwickler ein Software-Modul beispielsweise in Kopie „ausleiht“ und um neue Funktionen erweitert, führt ein anderer Entwickler im Original kurzfristig erforderliche Korrekturen (hot fixes) durch. Wird eine Synchronität nicht erzwungen, so können beide Versionsstände mit dem genannten Effekt auseinander laufen.



*Single-
Author-
Konzept,
Check-out-
check-in-
Prozedur*

Durch ein „Single-Author“-Konzept, verbunden mit einer geeigneten „Check-out-check-in“-Prozedur, die beim „Check-in“ eine Konsolidierung der Modulvarianten erzwingt, kann diesem Problem entgegengewirkt werden.

Änderungen in Software-Modulen sollten außerdem mit einer Referenz zur Änderungsanforderung und gegebenenfalls dem auslösenden Problem versehen sein, damit die erfolgten Änderungen jederzeit nachvollziehbar sind.



GAU durch Software-Update

Laut Zeitschrift CIO spielte das britische Department for Work and Pensions (DWP) am 22. November 2004 ein Routine-Upgrade von Windows® auf, als das gesamte System kollabierte. 80 % der 100.000 Rechner der Verwaltung waren in der Folge nicht mehr nutzbar. Angenommen wird, dass der Crash durch die Installation eines inkompatiblen Systems verursacht wurde. [Zeller, Thomas: Update führt zum IT-Super-Gau, CIO – News & Meinungen, 29.11.2004, 17:07]

*Patch-
management*

Ein Spezialfall des Änderungsmanagements ist das Patchmanagement. Seit Anfang der 2000er Jahre gewinnt es an Bedeutung aufgrund der zunehmenden Angriffe durch bösartigen Code und der

immer wieder auftretenden Schwachstellen in Betriebssystemen. Gleichzeitig hat sich die Zeit zwischen dem Erkennen einer Sicherheitslücke und deren Ausnutzung immer weiter verringert. Verschärft wird die Situation durch die zunehmende Mobilität der IT-Nutzer und deren Equipment. Was ist zu tun?

Absturz durch fehlenden Patch



Laut Zeitschrift CIO fiel das Check-in-System der Lufthansa am 2. Dezember 2004 morgens um 4:30 Uhr aus. Das Bodenpersonal musste die Bordkarten von Hand ausfüllen. Im innereuropäischen Linienverkehr wurden 60 Flüge gestrichen, Fluggäste mussten mehrere Stunden warten.

Bei der Umstellung der Plattentechnologie auf Glasfaser entstand beim letzten Change, bei dem auch das Check-in-System beteiligt war, ein Totalausfall. Das Zurückversetzen in den Ursprungszustand scheiterte, weil ein Patch für die fehlerhafte Software-Routine fehlte.

[Möhler, Tanja: Abstürze vermeiden, CIO, 12/2004, S. 54ff.]

Je nach Unternehmen übernimmt eine Person oder ein Team die Aufgabe, sicherheitsrelevante Informationen der Produkthersteller sowie deren Informationen zu Patches zu sichten. Eine weitere Aufgabe besteht darin, vertrauenswürdige Webseiten mit sicherheitsrelevanten Informationen kontinuierlich zu sichten bzw. sich über Mailings informieren zu lassen. Der Verantwortliche entscheidet in Abhängigkeit von der Gravität der Schwachstelle und der Kritikalität der Anwendung und Daten über die Priorität des jeweiligen Patches. Bei Relevanz stellt der Patchmanager eine Änderungsanforderung, die den Prozess des Änderungsmanagements mit entsprechender Priorität und Schnelligkeit durchläuft.

Parallel hierzu werden die Software-Updates, die eingespielt werden sollen, beschafft. Dies beinhaltet die Verifizierung, dass der Software-Update integer ist, also nicht absichtlich oder versehentlich verändert wurde. Dies kann über eine digitale Signatur oder geeignete Prüfsummen erfolgen.

Weiterhin ist es Aufgabe der Verantwortlichen, bei Updates für Arbeitsplätze die Verteilung (Roll-out) des Patches so zu planen, dass Komplettausfälle vermieden und das User Help Desk nicht überlastet werden.

Unter Kosten-Nutzen-Aspekten ist zu bewerten, ob die Anschaffung und der Einsatz eines geeigneten Patchmanagement-Tools wirtschaftlich ist. Das Tool sollte den detaillierten Patch-Level der Zielgeräte ermitteln, die Verteilung vornehmen und den Status verfolgen. Für nicht angeschlossene mobile Endgeräte sollte der Patch bereitgestellt

*Patch-
management-
Tool*

werden können. Außerdem sollte ein Rollback auf einen früheren stabilen Zustand möglich sein, falls der neu eingespielte Patch trotz erfolgreicher Abnahme Fehler oder Ausfälle verursacht. Das Tool sollte Berichte erzeugen, die den detaillierten Patch-Level der Zielgeräte dokumentieren.

9.5.12 Releasemanagement (Release Management)

Das Releasemanagement beschreibt, wie und wann (zeit- und ereignisgesteuert) Releases erstellt werden und welche Voraussetzungen für den Programmeinsatz erforderlich sind. Wesentliche Prozessschritte sind der Test, die Freigabe und gegebenenfalls die (zuvor getestete) Verteilung des Release. Im Vorfeld der Einführung sind darüber hinaus Überlegungen zum spätesten Rückfallzeitpunkt und zu den Rückfallmöglichkeiten erforderlich, falls Probleme auftreten. Das „Einfrieren“ und sichere Archivieren der Konfigurationselemente, die dem Release zugrunde liegen, ist ebenfalls darzustellen.

9.5.13 Konfigurationsmanagement (Configuration Management)

Eine Voraussetzung für den geordneten und damit in dieser Hinsicht sicheren Betrieb der ITK ist der Überblick über die eingesetzten Ressourcen, deren jeweilige Sicherheitsklasse je Sicherheitskriterium und deren Konfiguration sowie ihre Beziehungen zueinander (Interdependenzen) während des gesamten Lebenszyklus. Hierzu dient das Konfigurationsmanagement. Es umfasst u. a. die Prozesslandschaft und die genutzten Prozesse (Processware), Ressourcen, wie Systeme und Produkte, bestehend aus Hardware und Software, sowie die Dokumente und Dokumentationen (Paperware). Konfigurationsmanagement ist darüber hinaus auch bei der Verwaltung der Personalprofile gefordert.

Beispiele

In der folgenden Liste finden Sie zu verschiedenen Oberbegriffen Beispiele für Konfigurationselemente:

- Hardware (Systeme, Computer, Speichereinheiten, Netzkomponenten, Firewalls, Drucker)
- Software (jeweiliger Release von Anwendungen, Datenbanken, Betriebssystemen, Tools)
- Processware (Prozessbeschreibungen von Kern-, Unterstützungs- und Begleitprozessen)
- Paperware (Konzepte, Spezifikationen, Handbücher und Pläne z. B. von Gebäuden, haustechnischer Infrastruktur, Systemen, Rechnern, Entwicklungssystemen und -werkzeugen, Datenbanken, Kommunikationssoftware und Betriebssystemen sowie gegebene

nenfalls Quellcode. Ferner Verträge {Dienstleistung, Leasing, Wartung, Lizenz, Versicherung}, Service und Operational Level Agreements, Vollmachtenregelungen, Dienstleistungs- und Produktdaten, bis hin zu Weiterbildungsmaßnahmen und Qualifikationsprofilen von Mitarbeitern)

Durch entsprechende Prozesse, Verantwortlichkeiten, Hilfsmittel und Werkzeuge verschafft das Konfigurationsmanagements den Überblick über die Konfigurationselemente und ihren aktuellen Versions- und Releasestand. Doch wie lässt sich die Vielzahl der Konfigurationselemente und deren kontinuierliche Veränderung erfassen und für die Beteiligten zugreifbar gestalten?

Hier helfen Inventarisierungstools, manuelle Inventarisierung und eine historisierende Konfigurationsdatenbank weiter. Jedes Konfigurationselement muss dabei nach einer vorgegebenen Namenskonvention eindeutig identifiziert sein. Weitere Informationen beschreiben die aktuelle Version des Elements, das Datum, den Verantwortlichen und den Zusammenhang mit anderen Konfigurationselementen. Über einen Bezug zu einer Änderungsanforderung kann auf die Beschreibung der vorgenommenen Änderung zugegriffen werden.

*Konfigurations-
datenbank,
Namens-
konvention*

Anhand dieser Informationen lässt sich ermitteln, aus welchen Konfigurationselementen sich ein Informationssystem zusammensetzt und welche Version die einzelnen Elemente haben. Bei Hardware, z. B. einem Notebook lassen sich die installierten Hardware- und Softwarekomponenten sowie deren Releasestand herausfinden. Dies ermöglicht zielgerichtete Problemanalysen.

Es empfiehlt sich, den verschiedenen Funktionen und Rollen eines Unternehmens zuzuordnen, welche Software und Hardware, d. h. welche Konfigurationselemente, zur Aufgabenerfüllung erforderlich sind. So ergeben sich Standardkonfigurationen für Rollen und Arbeitsplätze, sogenannte Konfigurationscluster, z. B. für den Arbeitsplatz eines Sachbearbeiters in der Personalabteilung und in der Kreditbearbeitung, eines Administrators, eines Devisenhändlers, etc. Insbesondere beim Wechsel des Arbeitsplatzes innerhalb des Unternehmens ist aus Gründen der Sicherheit und Wirtschaftlichkeit (z. B. Lizenzkosten) darauf zu achten, dass die Konfiguration der neuen Rolle entsprechend angepasst wird.

*Konfigurations-
cluster*

9.5.14 Lizenzmanagement (Licence Management)

Der Bereich Informationsservices eines Unternehmens betreibt eine Vielzahl von Informationssystemen und Büroanwendungen, deren Nutzung lizenzrechtlichen Bestimmungen unterliegt. Kontinuierlich verändert sich die Zahl der Nutzer, neue kommen hinzu, andere

verlassen das Unternehmen oder wechseln in andere Bereiche mit anderen Aufgabenstellungen. Um den Überblick zu wahren, müssen die vorhandenen, die aktuell benötigten und die zukünftig erforderlichen Lizenzen und ihre Nutzungsbestimmungen bekannt sein. Das Lizenzmanagement stellt daher einen wesentlichen Bestandteil des ordnungsmäßigen Betriebs der Informationsverarbeitung dar.

Für den Aufbau des Lizenzmanagements sind u. a. folgende Informationen erforderlich: Produktname, Release, Anzahl der Lizenzen, Lizenznummern, Lizenzbedingungen. Diese müssen in Beziehung gesetzt werden zu den Geräten, auf denen sie installiert sind, sowie zu den Benutzern.

Der Überblick über die eingesetzte Software, beispielsweise für Textverarbeitung, Tabellenkalkulation, Präsentationen und zur HTML-Seitenerstellung, ermöglicht es, diese bei Bedarf zu konsolidieren und gegebenenfalls Einsparpotenziale zu heben. Die Gegenüberstellung von installierten und erworbenen Lizenzen erlaubt ebenfalls Einsparungen, wenn mehr Lizenzen vorhanden als installiert sind, so dass Bedarf und Bestand aneinander angeglichen werden.

Der Bereich Informationsservices sollte die eingesetzten Rechnersysteme in regelmäßigen Abständen überprüfen, um sicherzustellen, dass nur lizenzierte Software-Produkte im Einsatz ist. Die Prüfungen sollte er nachvollziehbar dokumentieren.

Mit den Nutzern sollte er eine Vereinbarung treffen, z. B. im Rahmen einer ITK-Benutzerordnung, die es ihnen untersagt, selbst Software auf geschäftlichen Systemen zu installieren.

Nutzungsanalysen geben Auskunft darüber, in welchem Umfang Software-Produkte an welchem Arbeitsplatz genutzt werden. Dies kann der Bereich Informationsservices zu Optimierungen im Lizenzmanagement nutzen.

9.5.15 Kapazitätsmanagement (Capacity Management)

Um die Verfügbarkeitsanforderungen eines Unternehmens und seiner ITK zu erfüllen, müssen für den Betrieb die benötigten Geschäfts- und Supportprozesse sowie die Ressourcen im erforderlichen Umfang und mit der geforderten Leistungsfähigkeit (Performance) zur Verfügung stehen. Hiermit beschäftigt sich das Kapazitäts- und Performancemanagement.

*Anforderungen
und
Ressourcen*

Ausgangspunkt des Kapazitäts- und Performancemanagements sind die Anforderungen der Kunden des Unternehmens. Aus ihnen leitet sich der jeweilige Kapazitäts- und Leistungsbedarf der Geschäfts-, Support- und Begleitprozesse sowie der genutzten Ressourcen ab.

Die Kapazität und Performance der Prozesse und Ressourcen ergibt sich z. B. aus der Anzahl von Transaktionen und aus dem Datenaufkommen sowie aus dem geforderten Durchsatz, der Durchlauf-, Antwort- und Reaktionszeit.

Diese Kapazitäts- und Leistungsanforderungen werden in den Leistungsvereinbarungen festgehalten und anschließend auf die ITK-Dienste, -Prozesse und die erforderlichen Ressourcen abgebildet. Zu den Ressourcen gehören folgende Objekte:

- Hardware (Kapazität und Leistungsfähigkeit)
 - Computer, z. B. Notebooks, PCs, Server, Großrechner
 - Netzkomponenten: aktive (z. B. Brücken, Router und Gateways) und passive (z. B. Verkabelung für LANs, SANs und WANs)
 - Peripherie
 - Eingabemedien, z. B. Scanner
 - Speichermedien, z. B. Cache, RAM, Festplatten, Bandbibliotheken
 - Ausgabemedien, z. B. Drucker, Druckstraßen und Kuvertiersysteme
- Software, z. B. Anzahl und Leistungsfähigkeit der Computer- und Netzbetriebssysteme, Datenbanken, gekauften Anwendungen, wie z. B. Office-Pakete, aber auch die Leistungsfähigkeit selbst entwickelter Anwendungen
- Personal, z. B. für den ITK-Bereich
- Externe Dienstleistungen bis hin zur Lizenzanzahl und zum Umfang von Versicherungen
- Externe Produkte.

Das Kapazitäts- und Performancemanagement umfasst entlang dem Lebenszyklus eines Prozesses oder einer Ressource die folgenden Elemente:

- Regelmäßige Erhebung und Pflege der aktuellen und zukünftigen Anforderungen (requirements)
- Beobachtung und Abschätzung technologischer Entwicklungen und Erfahrungen sowie Simulation der Auswirkungen
- Planung
- Konzeption (Anforderungsspezifikation, technische Spezifikation)
- Realisierung, Entwicklung
- Test, Freigabe und Abnahme
- Inbetriebnahme

- Überwachung (Monitoring), Analyse und Optimierung (Tuning) der Auslastung und des Durchsatzes, z. B. CPU- und Speicherauslastung sowie -Durchsatz
- Berichtswesen (reporting).

Nach der Festlegung, wer das Kapazitätsmanagement verantwortet, welche Aufgaben dazu gehören und welches Wissen dafür erforderlich ist, definiert der dafür ernannte Kapazitätsmanager, welche Tools zum Einsatz kommen, z. B. zum Monitoring. Zur Früherkennung von Engpässen legt der Kapazitätsmanager Schwellwerte für Warn- und Alarmgrenzen fest, z. B. hinsichtlich der Auslastung von Prozessen und Ressourcen, wie CPU, Platten, Drucker und Netz.

9.5.15.1 Rechnermanagement

Für den anforderungsgerechten Betrieb müssen die Rechner im Hinblick auf Antwortzeitverhalten und Kapazität ausreichend dimensioniert sein. Nach der Planung und Inbetriebnahme sollte das Antwortzeitverhalten und die Auslastung kontinuierlich überwacht, analysiert und optimiert werden.

9.5.15.2 Speichermanagement (Storage Management)

Daten sind ein zentraler Bestandteil der Betriebssicherheit. Dementsprechend müssen ihre anforderungsgerechte Verfügbarkeit sichergestellt und ausreichende Speicherkapazität bereitgestellt werden. Hierzu dient das Speichermanagement. Es erfordert Kenntnisse der verschiedenen Speichermöglichkeiten und ihrer Vor- und Nachteile. Detailliertere Ausführungen hierzu finden Sie im Kapitel Sicherheitsarchitektur unter Ressourcen.

9.5.16 Wartungsmanagement (Maintenance Management)

Das Wartungsmanagement beschreibt den Prozess der Wartung von Ressourcen, wie z. B. technischen Einrichtungen, Systemen oder Produkten. Hierbei werden die Wartungsobjekte identifiziert und zusammen mit ihren Wartungsintervallen, Wartungsfenstern, Verantwortlichen und gegebenenfalls den Wartungsunternehmen erfasst. Je nach Sicherheitsanforderungen und Komplexität des jeweiligen Wartungsobjekts ist das Verfahren für die Wartung angemessen detailliert zu beschreiben, damit Fehler während der Wartung möglichst vermieden werden. In der Beschreibung ist zu berücksichtigen, dass das Wartungsobjekt, z. B. eine USV, während des Wartungsfensters nicht zur Verfügung steht. Ein Stromausfall während der Wartung

hat somit direkte Auswirkungen, wenn die USV nicht redundant ausgelegt und mit geeigneter Umschaltung versehen ist.

Sicherheitstechnisch relevante Wartungsobjekte sind beispielsweise Gefahrenmeldeanlagen, die NEA und die USV einschließlich der Batterien. Die NEA beispielsweise sollte regelmäßig gewartet und monatlich nachvollziehbar auf Funktionsfähigkeit getestet werden. Hierzu gehört auch die Sicherstellung, dass für den Notfall ausreichend Brennstoff zur Verfügung steht. Regelmäßige Wartung und Prüfung ist auch für die USV, die Batterie und deren Leistung relevant.

*Wartungs-
objekte*

Ein weiterer Aspekt im Wartungsmanagement ist die präventive Wartung (preventive/preemptive maintenance), bei der z. B. Sicherungsdatenbänder und -disketten vor Ablauf ihrer durchschnittlichen Lebenserwartung präventiv ausgewechselt werden. Ein geeignetes IT-System kann auf anstehende Wartungen und Abhängigkeiten bei fehlschlagenden Wartungen aufmerksam machen sowie die Ergebnisse, d. h. die Wartungsprotokolle, verwalten. Die Wartungsprotokolle enthalten Angaben darüber, wer wann welche Wartungstätigkeiten mit welchem Ergebnis durchgeführt hat und wann die nächste Wartung ansteht.

*Präventive
Wartung*

Als wesentliche und für die Sicherheit wichtige Elemente des Wartungsprozesses sind ferner die Auswahl der Wartungsunternehmen, die Vertragsgestaltung und die Einweisung der Mitarbeiter des Wartungsunternehmens anzusehen.

9.5.17 Kontinuitätsmanagement (Continuity Management)

Ursachen für Ausfälle und Störungen der Informations- und Kommunikationsinfrastruktur sind vielfältig. Der Ausfall einer Festplatte infolge eines Headcrashes, der Ausfall einer Kommunikationseinrichtung oder der Brand eines Rechenzentrums oder Serverraums führen – ohne entsprechende Absicherungen – zu einem Ausfall der Informationsverarbeitung. Auch das versehentliche Betätigen des ungeschützten RZ-Notausschalters hat diese Folgen.

*Ursachen für
Ausfälle und
Störungen*

Gleiches gilt für den Ausfall von Mitarbeitern, die über nicht ausreichend dokumentiertes oder undokumentiertes Spezialwissen verfügen und keinen gleich kompetenten Vertreter haben. Derartige Ausfälle schränken die Handlungsfähigkeit des Unternehmens oder einer Organisationseinheit ohne entsprechende Absicherung mehr oder weniger stark ein.

*Prävention,
Regeneration
und
Postvention*

Um dies den Sicherheitsanforderungen entsprechend zu vermeiden oder abzumildern, müssen die Verantwortlichen Maßnahmen ergreifen, die dem Eintreten oder den Auswirkungen eines Notfalls oder einer Katastrophe entgegenwirken. Derartige Maßnahmen sollen einerseits präventiver Natur sein, indem sie von vornherein Ausfälle z. B. durch menschliches Versagen so weit wie möglich verhindern. Außerdem müssen so genannte „Single Points of Failure“ vermieden werden, d. h. Stellen, bei deren Ausfall es keine Ausweich-/Ersatzmöglichkeit gibt. Positiv formuliert bedeutet dies, dass für jedes Element des Gesamtsystems mindestens ein Ersatz oder eine Ausweichmöglichkeit vorhanden sein muss, d. h. dass diese Elemente in geeigneter Form redundant vorhanden sind.

Andererseits sind geeignete Maßnahmen erforderlich, um nach einer Katastrophe in vordefinierter Zeit den – oftmals reduzierten – Not- oder idealerweise regulären Betrieb wieder aufzunehmen. Dies beinhaltet den Übergang in den Notbetrieb, den Notbetrieb, die Wiederherstellung (Regeneration) der betroffenen Ressourcen und Dienste sowie die Rückkehr aus dem Notbetrieb in den regulären Betrieb samt Nacharbeiten (Postvention).

*Präventiv-
maßnahmen*

Die Präventivmaßnahmen lassen sich unterscheiden in solche, die getroffen werden, bevor das System in Betrieb genommen wird, und solche, die im Betrieb einen störungsfreien, fehlervermeidenden Ablauf unterstützen. Als Maßnahme vor der Inbetriebnahme ist hier z. B. der Systemtest, d. h. der Test des Gesamtsystems mit allen beteiligten Komponenten zu nennen. Wie verhält sich das System beispielsweise, wenn eine Festplatte ausfällt, der Router streikt, oder der Strom mitten in einer Transaktion ausfällt? Wie robust ist das System gegenüber Fehlbedienungen des Benutzers? Inwieweit lässt es Fehlbedienungen überhaupt zu? Im Rahmen eines ausgiebigen Systemtests können Sie bereits tiefgehende Erkenntnisse über die Betriebssicherheit des Systems und das Systemverhalten bekommen.

Aber ist dies nicht bereits zu spät? – Was ist, wenn Sie feststellen, dass das System zwar hoch verfügbar sein soll und der Inbetriebnahmezeitpunkt feststeht, das System aber unzureichende oder gar keine Vorsorge für die Betriebssicherheit getroffen hat? – Sie befinden sich dann in einer ähnlichen Lage wie die Industrie, als sie erkannte, dass die Endabnahme letztlich nur noch feststellt, ob das Produkt in Ordnung oder Ausschuss ist. Sicherlich, dazwischen gibt es noch eine Vielzahl von Ergebnisschattierungen. Bei diesen wird dann versucht, z. B. durch Nacharbeiten, das geforderte Qualitätsniveau doch noch zu erreichen. Letztendlich führt dies jedoch stets zu Zusatzarbeiten.

Industrieunternehmen haben hieraus gelernt, dass der Fertigungsprozess kontinuierlich überwacht werden muss, um bei Fehlentwicklungen zum frühest möglichen Zeitpunkt gegensteuern zu können. Außerdem müssen alle Beteiligten – vom Vertrieb über den Einkauf, die Fertigung und das Controlling bis hin zur Forschungs- und Entwicklungsabteilung – in eine Neuentwicklung, d. h. in den Entwicklungsprozess mit einbezogen werden.

*Beispiel
Industrie*

Die kontinuierliche Überprüfung und Steuerung kennen Sie sicherlich auch aus der Software-Entwicklung. Aufgrund der Komplexität und der Erkenntnis, dass die Kosten für Fehler drastisch ansteigen, je später sie erkannt werden, legen erfahrene Projektmanager hier besonderen Wert auf Reviews, Code-Inspektionen, Modul-, Komponenten- und Systemtests. Dies sind Maßnahmen, die im Vorfeld des Abnahmetests und entwicklungsbegleitend stattfinden.

Je nach Umfang können die Präventivmaßnahmen somit helfen, Ausfälle nicht zu Notfällen oder Katastrophen werden zu lassen. Dennoch wird es weiterhin Notfälle und Katastrophen geben können. Diese gilt es durch einen entsprechenden Notfall- und Katastrophenvorsorgeplan (Business Continuity Plan einschließlich Disaster Recovery Plan) abzusichern.

Lassen Sie mich bezüglich der Präventivmaßnahmen zusammenfassen: Sicherheitsanforderungen müssen über alle Phasen des Lebenszyklus eines Prozesses, einer Ressource, einer Dienstleistung und eines Produkts definiert, verfeinert, verfolgt und gesteuert sowie in diese integriert werden. Durch diese lebenszyklus- sowie prozess-, ressourcen-, (dienst)leistungs- und produktimmanente Sicherheit lässt sich erreichen, dass die Sicherheitsanforderungen erfüllt werden können.

*Lebenszyklus-
immanente
Sicherheit*

Unter Berücksichtigung der Lebenszyklusimmanenz hat das Kontinuitätsmanagement die Aufgabe, die geforderte Verfügbarkeit der ITK-Systeme und -Dienste im regulären Betrieb so zu erreichen, dass trotz eines Notfalls oder einer Katastrophe eine angemessene Handlungsfähigkeit des Unternehmens erhalten bleibt. Das Kontinuitätsmanagement umfasst folgende Aktivitäten:

*Kontinuitäts-
management*

1. die regelmäßige und frühzeitige Erhebung und Aktualisierung der Mindestszenarien, Prinzipien und Bedrohungen
2. die regelmäßige und frühzeitige Erhebung und Aktualisierung der Verfügbarkeits- bzw. Kontinuitätsanforderungen
3. die Bildung von Verfügbarkeits- bzw. Kontinuitätsklassen

4. die Planung der Verfügbarkeit, z. B. durch Absicherungen in Form von Redundanzen, Datensicherung sowie Notfall- und Katastrophenvorsorge bis hin zur Versicherung von Risiken
5. das Review und den Test der festgelegten Verfahren und Maßnahmen
6. die Schulung und regelmäßige Übung der definierten Verfahren
7. die Messung, Analyse und Optimierung der Verfügbarkeit
8. die Erstellung von Berichten.

Die Anforderungen an die Verfügbarkeit werden wesentlich mit bestimmt von den Kosten, die durch die Ausfallzeit entstehen. Hierbei sind folgende Fragen zu berücksichtigen:

- Wie lange darf das ITK-System bei einem Ausfall maximal nicht verfügbar sein?
- Wie lange darf das ITK-System pro Jahr insgesamt maximal ausfallen?
- In welchem minimalen zeitlichen Abstand darf das System erneut ausfallen?



Hohe Ausfallkosten

Laut [32] rangieren die stündlichen Ausfallkosten von ITK-Systemen für den Börsenhandel, Telekommunikationsunternehmen und die Kreditkartenabwicklung an oberster Stelle. Eine Stunde Ausfallzeit kostet hier zwischen 7,8 Mio. \$ und 3,2 Mio. \$. Eine Ausfallzeit von knapp einer Stunde entspricht einer Verfügbarkeit von 99,99 % pro Jahr.

Die Verfügbarkeit pro Jahr wird häufig in Prozent angegeben. Anhand der Prozentangaben lassen sich die maximalen Ausfallzeiten (Downtime) pro Jahr errechnen, die in der folgenden Tabelle gerundet angegeben sind. Als hochverfügbar bezeichne ich Lösungen ab einer maximalen Ausfallzeit von 1 h pro Jahr.

*Vermeidung
durch
Prävention*

Der Bereich Informationsservices muss die ITK-Systeme entsprechend den Verfügbarkeitsanforderungen und Kosten-Nutzen-Überlegungen angemessen absichern. Durch eine Pfadanalyse kann er ermitteln, welche „Single Points of Failure“ existieren, welche Folgen ein Ausfall hat und welche Alternativen bei einem Ausfall bestehen. Auf dieser Basis lassen sich Entscheidungen gegen oder für eine redundante Ausgestaltung sowie deren Umfang treffen, oder andere Absicherungen vornehmen.

Verfüg- barkeit in Prozent	Max. Ausfallzeit pro Jahr, gerundet in Abhängigkeit von der Betriebszeit			Bezeichnung
	7 Tage x 24 h	7 Tage x 12 h	5 Tage x 12 h	
99,0	4 Tage	2 Tage	1,5 Tage	
99,5	2 Tage	1 Tag	16 h	
99,9	9 h	5 h	3 h	Verfügbar
99,99	1 h	0,5 h	0,3 h	Hochverfügbar
99,999	6 min	3 min	2 min	Höchstverfügbar
99,9999	32 sec	16 sec	11 sec	Unterbrechungsarm
...	...	...		...
100	0 sec	0 sec	0 sec	Kontinuierlich verfügbar, unterbrechungsfrei

Daten sind der wesentliche Kernpunkt der Informationssysteme. Somit stellt die regelmäßige Datensicherung ein grundlegendes Sicherheitselement dar. Bei einem Datenverlust, z. B. aufgrund eines Plattencrashes oder bei Datenverfälschungen aufgrund eines Software-Fehlers können die Daten auf diesem Wege bis zum Zeitpunkt der letzten Sicherung restauriert werden.

Datensicherung

Um auch frühere Zustände wiederherstellen zu können oder trotz eines defekten Datenträgers auf einem möglichst zeitnahen Zustand wieder aufsetzen zu können, müssen Daten in mehreren „Generationen“ gesichert und aufbewahrt werden. Damit lokale Katastrophen, wie z. B. ein Brand, nicht auch gleichzeitig die Datenträger vernichtet, müssen diese ausgelagert werden, z. B. in ein räumlich ausreichend getrenntes und geschütztes Datenträgerarchiv.

*Generationen-
sicherung,
deren
Aufbewahrung
und
Auslagerung*

Ein weiteres Element zur Absicherung der Verfügbarkeit ist die Notfall- und Katastrophenvorsorgeplanung. Sie beschreibt u. a. prinzipielle Katastrophenszenarien und die dazugehörigen Reaktionen.

*Notfall- und
Katastrophenvorsorge*

Damit das Vorgehen für den – wie ich es differenziert nenne – Übergang in den Notbetrieb, den Notbetrieb und die Rückkehr in den regulären Betrieb möglichst reibungslos klappt, ist eine entsprechende Dokumentation des Vorgehens erforderlich. Die Verantwortlichen müssen die Dokumentation aktuell halten. Eine alternative, aber meist undifferenzierte Bezeichnung für den Übergang in und die Rückkehr aus dem Notbetrieb ist der Begriff Wiederanlauf (recovery). Den Übergang in den Notbetrieb und die Rückkehr in den regulären Betrieb müssen die Beteiligten ebenso wie den Notbetrieb selbst in regelmäßigen Abständen üben. Dies erfordert eine geeignete Planung und Vorbereitung sowie Protokollierung und Auswertung.

*Übergang in
den Notbetrieb,
Notbetrieb,
Rückkehr in den
regulären
Betrieb*

Für den realen Fall, aber auch für die Übungen, eignen sich beispielsweise Checklisten, die ein nachvollziehbares „Abhaken“ (Datum, Uhrzeit, Signatur, Bemerkung) durchgeführter Aktivitäten ermöglichen und die Übergabe bei Schichtwechsel unterstützen. Alternativ lassen sich datenbankbasierende Tools oder Text und Datenbank integrierende Tools nutzen.

*Sicherheits-
elemente
Notfall- und
Katastrophen-
vorsorge*

Unter dem Aspekt der Notfall- und Katastrophenvorsorge ergeben sich für die Betriebssicherheit folgende Sicherheitselemente:

1. Prävention zur Vermeidung von Störungen und Problemen
2. Datensicherung einschließlich deren Umfang, Zeitpunkt, Aufbewahrung und Auslagerung zur Verringerung der Auswirkung von Datenverlusten
3. Notfall- und Katastrophenvorsorgeplanung einschließlich Wiederanlaufverfahren zur Verringerung der Auswirkungen von Notfällen und Katastrophen
4. Versicherungen zur Verlagerung von Risiken.

9.5.17.1 Vermeidung durch Prävention

Um herauszufinden, welche Sicherheitselemente zur Absicherung der ITK eingesetzt werden können, wird im Folgenden analysiert, aus welchen Komponenten sich die ITK selbst, die erforderliche Infrastruktur und ihr Umfeld, wie z. B. Räumlichkeiten und Gebäude, zusammensetzen.

*ITK,
Infrastruktur
und Umfeld*

Ausgangspunkt ist das äußere Umfeld des Unternehmens, die externen Versorgungseinrichtungen und die Service-Geber. Hieran schließt sich das Gebäude und die Räumlichkeiten sowie die jeweilige Infrastruktur an. Schließlich gelangen wir zur ITK in Form von Rechnern, Hardware-Komponenten und Software. Häufig unbeliebt, aber stets wichtig, ist die jeweilige Dokumentation.

*Umfeld und
Lage des
Gebäudes*

Was hat das äußere Umfeld mit der Betriebssicherheit zu tun? Hierzu sehen wir uns die Lage des Gebäudes an. Es kann in der Einflugschneise eines Flughafens liegen, direkt neben einer Hauptverkehrsstraße oder an einem Rangierbahnhof, neben einer Tankstelle oder einem Chemieunternehmen oder auch direkt an einem Fluss. Neben dem Gebäude kann unterhalb der Erdoberfläche eine U-Bahn verlaufen, von der Vibrationen ausgehen. Ein Element der Sicherheitsarchitektur besteht daher in der Lage des Gebäudes bzw. der Absicherung gegenüber dem Umfeld. Hierfür sind in der nächsten Ebene der Sicherheitspyramide, den Sicherheitsrichtlinien, entsprechende Vorgaben zu machen.

Die Anbindung des Gebäudes an das Umfeld, d. h. die Versorgung, ist als Nächstes zu betrachten. Versorgungseinrichtungen, wie z. B. Strom, Wasser, Gas und Kommunikation müssen den Sicherheitsanforderungen entsprechend abgesichert werden. Hier kommt das Prinzip der Redundanz zur Anwendung. Beispielsweise kann die Stromversorgung durch redundante und räumlich getrennte Anbindung an das öffentliche Netz, durch eine Unterbrechungsfreie Stromversorgung (USV) und gegebenenfalls eine Netzersatzanlage (NEA) abgesichert werden. Bei der eigenen Absicherung sind auch die Verträge mit den Versorgungsunternehmen und die dort zugesicherten Leistungen und deren Verfügbarkeit einzubeziehen. Je nach Sicherheitsanforderungen ergeben sich beispielsweise für die Absicherung der externen Stromversorgung als Architekturelemente eine redundante Netzanbindung, NEA, USV und entsprechende Verträge mit dem bzw. den Stromversorgern.

*Externe
Versorgung*

Leistungen, die von Service-Gebern, wie z. B. Lieferanten und Outsourcing-Unternehmen, bereit gestellt werden, muss der Service-Nehmer durch entsprechende Service-Level-Agreements vertraglich fixieren. Durch Vorgaben zur Auswahl und kontinuierlichen Bewertung eines Service-Gebers und zum Aufbau von Alternativen, z. B. durch Verträge mit mehr als einem Lieferanten, können diese abgesichert werden.

*Externe
Dienstleister,
Service-Geber*

Für die Bauweise und die Gestaltung des Gebäudes sowie dessen Infrastruktur sollte ein Unternehmen entweder Vorgaben machen oder sich anderweitig gegen Bedrohungen absichern. Beispielsweise sollten äußere Fensterbänke im Erdgeschoss so geneigt sein, dass sich darauf keine Objekte abstellen lassen.

*Gebäude und
Infrastruktur*

Bei der Infrastruktur sollte das Unternehmen bzw. sein IT-Bereich je nach Sicherheitsanforderungen z. B. auf redundante und räumlich getrennte Verkabelung achten. Eine wesentliche Vorgabe ist darüber hinaus, dass die Dokumentation des Gebäudes (Bauzeichnungen/Baupläne) und seiner Infrastruktur vorhanden und aktuell sein muss. Weitere Schutzmaßnahmen betreffen Sprinkleranlagen, Brandabschnitte und Brandmeldeanlagen (BMA), auf die z. B. Rauchmelder an der Decke hinweisen.

Als Sicherheitselemente der Architektur lassen sich hieraus beispielsweise die sichere Gebäude- und Infrastrukturkonzeption sowie deren Dokumentation aufnehmen. Ihre konkrete Ausprägung findet sich u. a. in Bau- und Kabelplänen wieder.

Räumlichkeiten und Infrastruktur

Für die Ausgestaltung der Räumlichkeiten innerhalb des Gebäudes und deren Infrastruktur sind Vorgaben hinsichtlich Lage, Gestaltung, Ausstattung und Absicherung zu machen. Entsprechende gesetzliche Bestimmungen oder Ausführungsrichtlinien müssen beachtet werden. Je nach Zweckbestimmung unterscheiden sich die Anforderungen an die Räumlichkeiten, z. B. an Büroräume, Datenträgerarchive, Etagenverteiler, Technikräume, Serverräume und Rechenzentrum. Für diese werden Vorgaben entwickelt, die sich z. B. auf die Klimatisierung, den Brandschutz und Brandabschnitte sowie die Absicherung gegen Wasser einschließlich einer Wassermeldeanlage (WMA) beziehen.

In Abhängigkeit von den Verfügbarkeitsanforderungen sind darüber hinaus redundante Räumlichkeiten, z. B. verteilte Rechenzentren oder ein Ausweichrechenzentrum, redundante Technikräume etc. vorzusehen und entsprechende Konzepte zu entwickeln. Auch hier gilt, dass die Dokumentation der Räumlichkeiten und deren Infrastruktur vorhanden, für die Beteiligten gut zugänglich und aktuell sein muss.

In der Sicherheitsarchitektur wird festgelegt, welche Raumkategorien existieren, für die in der Folge unterschiedliche Sicherheitsrichtlinien entwickelt werden müssen. Kriterien hierfür sind z. B. die Sicherheitsanforderungen, der Kreis der Zutrittsberechtigten und der Zweck der jeweiligen Räumlichkeiten, z. B. Serverräume und Datenträgerarchive.

ITK- Infrastruktur

Kritische Informations- und Telekommunikationssysteme müssen entsprechend den Sicherheitsanforderungen geschützt sein, um Katastrophen möglichst zu vermeiden und Risiken zu verringern. Dies erfordert Vorgaben für Rechner, Hardware-Komponenten, Betriebssysteme, Rechteverwaltungssystem, Kommunikationssoftware, Datenbanken, Büroanwendungen und Informationssysteme. Diese beziehen sich beispielsweise darauf, dass die Anzahl der eingesetzten Betriebssysteme optimiert wird und die Betriebs- und Kommunikationssysteme so konfiguriert werden, dass sie nach dem Prinzip der minimalen Dienste nur die Dienste zur Verfügung stellen, die auch genutzt werden sollen. Darüber hinaus müssen in Abhängigkeit von den Verfügbarkeitsanforderungen Redundanzen geschaffen werden. Neben gesicherten Datenbeständen und gespiegelten Platten gibt es verschiedene Möglichkeiten, um die Verfügbarkeit der Rechnersysteme zu erhöhen:

1. Ersatzkomponenten
2. Ersatzrechner
3. Cluster-System
4. Fehlertolerante Rechner

Derzeit können Stand-alone-Server über Festplatten, PCI-Karten und Netzteile verfügen, die im laufenden Betrieb auswechselbar sind (hot pluggable). Hierdurch sind jedoch einerseits nicht alle Fehlersituationen behebbar und andererseits ist Zeit für den Wechsel, eventuelle Datenrücksicherungen etc. erforderlich.

*Ersatz-
komponenten*

Alternativ kann für den ausgefallenen Rechner ein Ersatzrechner bereit stehen. Auch hier fallen Zeiten z. B. für den Austausch, eventuelle Datenrücksicherungen und die Konfiguration an.

Ersatzrechner

Eine weitere Alternative stellen Cluster-Systeme dar. Hier sind zwei oder mehr Server (Knoten) physisch und per Software so miteinander verbunden, dass bei Ausfall eines Servers der andere dessen Aufgaben mit übernimmt. Der Aufbau eines Clusters erfordert im Vorfeld Aufwand, um das Cluster zu konfigurieren sowie die für den Ausfall erforderlichen Skripte zu entwickeln und zu testen. Diese müssen in der Folge bei Hardware- und Software-Änderungen gegebenenfalls gepflegt werden. Fällt ein Server aus, so übernimmt der Rest des Clusters seine Aufgaben, wobei die Daten im Hauptspeicher des defekten Servers verloren sind. Ebenfalls zu beachten ist, dass die Cluster-Software bzw. Cluster-Steuerung selbst einen potenziellen „Single Point of Failure“ darstellt.

Cluster

Die derzeit wohl redundanteste Lösung für Rechnersysteme stellen fehlertolerante Systeme dar. Hierbei kann es sich prinzipiell um reine Hardware-Lösungen oder um kombinierte Hard- und Software-Lösungen handeln. Bei reinen Hardware-Lösungen werden Verfügbarkeiten von 99,999 % angegeben [33]. Dies entspricht einer Ausfallzeit von ca. 5 min p. a. Bei derartigen Systemen ist Rechnerhardware dupliziert, z. B. CPU, Hauptspeicher, Festplatte, PCI-Karten und Netzteil. Die beiden CPUs und der Hauptspeicher arbeiten hierbei synchron, indem sie zeitgleich die gleiche Instruktion abarbeiten. Bei Ausfall einer redundanten Komponente setzt die intakte Komponente die Verarbeitung ohne Unterbrechung und ohne Verlangsamung fort. Die redundanten und im laufenden Betrieb wechselbaren (hot swappable) defekten Komponenten kann der Systembetreuer auswechseln.

*Fehlertolerante
Rechner*

Nicht vergessen werden sollten auch jene Mitarbeiter, die für den Betrieb der Informationssysteme zuständig sind. Hier ist Redundanz im Sinne kompetenter Stellvertreterregelungen wichtig.

Personal

Aufgrund der bisherigen Ausführungen ergeben sich folgende präventiv-vermeidende Sicherheitselemente:

*Sicherheits-
elemente*

- Umfeld und Lage des Gebäudes
- externe Versorgung
- externe Lieferanten und Dienstleister (Service-Geber)
- Gebäude und Infrastruktur
- Räumlichkeiten und Infrastruktur
- ITK-Infrastruktur.

9.5.17.2 Datensicherung

Trotz dieser präventiv-vermeidenden Maßnahmen kann es zu Fehlern und Ausfällen kommen, bei denen Datenträger zerstört oder in Mitleidenschaft gezogen werden. Hierbei können Daten verloren gehen. Damit diese im geforderten Umfang und mit der geforderten Zeitnähe wiederhergestellt werden können, werden Datensicherungen durchgeführt. Bei der Datensicherung lassen sich folgende Themenstellungen unterscheiden:

1. Sicherungsmethoden
2. Sicherungszeitpunkt
3. Aufbewahrungsort
4. Auslagerungsverfahren

9.5.17.2.1 Sicherungsmethoden

*Sicherungs-
methoden*

Die Ausführungen zum Speichermanagement haben gezeigt, dass für die Datensicherung die Speichermedien und die Speichertopologie festgelegt werden müssen. Ein weiteres Element ist die Sicherungsmethode.

Bei den Sicherungsmethoden kann unterschieden werden in:

- komplette Datensicherung
- differenzielle Datensicherung
- inkrementelle Datensicherung
- selektive Datensicherung.

*Komplette
Datensicherung*

Eine komplette Datensicherung sichert den gesamten Datenbestand. Voraussetzung hierfür ist, dass der erforderliche Zeitraum zur Verfügung steht. Außerdem darf der Datenbestand innerhalb dieses Zeitraums nicht mehr verändert werden, um Inkonsistenzen zu vermeiden und dem Benutzer sagen zu können, welchen Zeitpunkt der Datenbestand reflektiert. Vorteil dieses Verfahrens ist die Möglichkeit der kompletten Rücksicherung, Nachteil der hohe Zeitbedarf der Sicherung und der hohe Verbrauch an Sicherungsmedien.

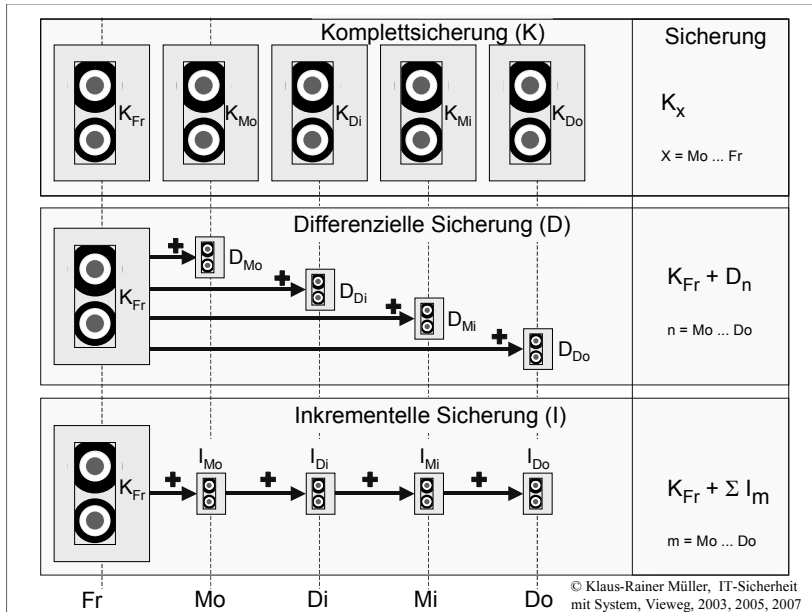


Abb. 9.6: Datensicherungsmethoden

Die differenzielle Datensicherung besteht aus:

1. einer kompletten Datensicherung zu Anfang
2. (mehreren) Folgedatensicherungen der Dateien, die sich gegenüber der Komplettsicherung verändert haben (Differenz zur Anfangssicherung)

*Differenzielle
Datensicherung*

Üblicherweise erfolgt die komplette Datensicherung an einem festgelegten Tag der Woche, während an den folgenden Wochentagen die hierzu veränderten Daten gesichert werden.

Vorteil der differenziellen gegenüber der kompletten Datensicherung ist, dass die Folgedatensicherungen ein kürzeres Zeitfenster und weniger Sicherungsmedien benötigen. Nachteilhaft ist die zweistufige und gegenüber der kompletten Datensicherung längere Rücksicherung. Nach dem Einspielen der Komplettsicherung müssen nämlich die danach veränderten Dateien von der differenziellen Datensicherung überspielt werden.

Die inkrementelle Datensicherung (Zuwachssicherung) beginnt mit

1. einer kompletten Datensicherung zu Anfang
2. (mehreren) Folgedatensicherungen der Dateien, die sich gegenüber dem vorherigen Sicherungslauf verändert haben.

*Inkrementelle
Datensicherung*

Die inkrementelle Datensicherung wird wie die differenzielle üblicherweise im Wochenrhythmus durchgeführt.

Vorteil dieser Methode gegenüber der kompletten Datensicherung sind kleine Zeitfenster für die Folgedatensicherungen und hierbei sparsamer Umgang mit den Sicherungsmedien. Nachteil ist, dass bei der Rückspeicherung die einzelnen Datensicherungen in der richtigen Reihenfolge sukzessive eingespielt werden müssen. Dies ist kompliziert und zeitaufwändig.

*Selektive
Datensicherung*

Bei der selektiven Datensicherung werden gezielt nur bestimmte Verzeichnisse oder ausgewählte Dateien gesichert.

*Vor- und
Nachteile der
Sicherungsmethoden*

Einen Überblick über die gegenseitigen Vor- und Nachteile der verschiedenen Methoden zur Datensicherung gibt die folgende Tabelle.

Sicherungsumfang	Zeitfenster		Medienverbrauch	Komplexität
	Sicherung	Rücksicherung		
Komplett	Groß	Klein	Hoch	Niedrig
Differenziell	Mittel	Mittel	Mittel	Mittel
Inkrementell	Klein	Groß	Niedrig	Hoch

Ein weiterer Unterschied der verschiedenen Datensicherungsmethoden besteht darin, dass der Defekt eines Datenbandes unterschiedliche Auswirkungen hat. Bei den Komplettsicherungen gehen bei Defekt eines Bandes im ungünstigsten Fall die Daten eines Tages verloren, bei der differenziellen ebenso wie bei der inkrementellen im ungünstigen Fall die einer Woche.

*Datensicherungs-
generationen*

Um sowohl unterschiedliche frühere Datenbestände wieder herstellen zu können als auch für Defekte an Sicherungsmedien gerüstet zu sein, sind mehrere Generation von Datensicherungen erforderlich. Hierdurch wird es ebenfalls möglich, Datensicherungen räumlich getrennt auszulagern, um für Katastrophen gerüstet zu sein.

*Urgroßvater-
Großvater-
Vater-Sohn-
Datensicherung*

Am bekanntesten dürfte das Urgroßvater-Großvater-Vater-Sohn-Wechselschema sein. Entsprechend der jeweiligen Generation gibt es Mediasets für die täglichen (Sohn), wöchentlichen (Vater), monatlichen (Großvater) und jährlichen (Urgroßvater) Datensicherungen.

Kennzeichnung

Die jeweiligen Mediasets werden ihrer Generation entsprechend mit den Tagen (Mo, Di, Mi, Do, Fr, Sa, So), den relativen Wochen für die erste bis fünfte Wochensicherung, den Monaten (Januar ... Dezember) und Jahren beschriftet. Darüber hinaus erhalten die Bänder eine Kennzeichnung, durch die sie eindeutig identifizierbar sind.

Bei den täglichen Sicherungen (Sohn) kommen üblicherweise inkrementelle Datensicherungen zum Einsatz, während die „älteren“ Generationen (Vater, Großvater, Urgroßvater) als Komplettsicherung durchgeführt werden. Die Wochensicherungen werden an einem festen Wochentag vorgenommen. Sie bilden den Ausgangspunkt für den nächsten Zyklus differenzieller oder inkrementeller Tagessicherungen.

9.5.17.2.2 Sicherungszeitpunkt

Nach Sicherungszeitpunkten der Datensicherung kann unterschieden werden in

1. Zeitversetzt (time delayed), z. B. einmal täglich
2. Zeitnah (neartime), z. B. asynchrone Spiegelung
3. Zeitgleich bzw. in Echtzeit (realtime), z. B. synchrone Spiegelung

Bei einem irreversiblen Defekt eines Datenspeichers sind die nach dem letzten Sicherungszeitpunkt veränderten Daten verloren. Demzufolge richtet sich der Sicherungszeitpunkt nach der Wichtigkeit der Daten und dem Aufwand für die Wiedergewinnung der Daten.

Zeitversetzte Datensicherungen werden periodisch zu einem bestimmten Termin, z. B. einmal täglich durchgeführt. Ein Beispiel hierfür ist die tägliche Sicherung auf Datenbändern.

*Zeitversetzte
Datensicherung*

Zeitnahe Datensicherungen erfolgen in einem zeitlichen Abstand von Sekunden bis hin zu wenigen Minuten. Ein Beispiel hierfür ist die asynchrone Datenspiegelung (asynchrone Replikation).

*Zeitnahe
Datensicherung*

Zeitgleiche Datensicherungen, d. h. Datensicherungen in Echtzeit, nutzen die Spiegelung, wobei die Schreibvorgänge erst dann bestätigt werden, wenn die synchrone Replikation erfolgreich abgeschlossen worden ist. Von „außen“ betrachtet werden die Originaldaten und das Replikat quasi gleichzeitig abgelegt. Sie werden entweder mit Abschluss einer Transaktion auf beiden Festplatten gleichzeitig oder gar nicht gültig.

*Echtzeit-
Datensicherung*

Die synchrone Spiegelung kann entweder die Anwendung selbst, eine entsprechende „Software-Utility“ oder die Festplatteneinheit selbst (in Form der Plattenspiegelung {Mirroring, RAID-Level 1}) durchführen.

*Synchrone
Spiegelung*

Bei einer synchronen Spiegelung schreibt entweder die Anwendung selbst oder eine „Software-Utility“ die Daten auf zwei getrennte Festplatteneinheiten. Die Daten einer Transaktion werden hierbei erst nach einem so genannten „Two-Phase-Commit“ gültig, d. h. wenn

*Software-
basierte
Spiegelung*

jede Speichereinheit die erfolgreiche Speicherung zurückgemeldet hat.

Nachteile

Der Nachteil einer Spiegelung durch die Anwendung besteht darin, dass die Anwendung diese Funktionalität aufweisen, d. h. entsprechend programmiert sein muss. Ein weiterer Nachteil ist darin zu sehen, dass die CPU bei einer softwaremäßigen Spiegelung durch die Anwendung oder durch eine „Software-Utility“ zusätzlich belastet wird.

Hardware- basierte Spiegelung

Bei hardwarebasierten Lösungen erfolgt die Spiegelung durch die Speichereinheit selbst.

Vorteile dieser Lösung sind darin zu sehen, dass die Anwendung

1. keine Zusatzfunktionalität für die Replikation der Daten besitzen muss,
2. die CPU dementsprechend nicht zusätzlich belastet wird
3. die hardwarebasierte Lösung eine bessere Performance aufweist.

Bei größerer räumlicher Distanz der Festplatten, z. B. von 10 km, hat jedoch auch eine solche Lösung Einfluss auf das Antwortzeitverhalten der Anwendung. Dies liegt z. B. darin begründet, dass die Daten per Datenübertragung zur zweiten Speichereinheit übertragen werden müssen und das „Commit“ der zweiten Speichereinheit abgewartet werden muss.

9.5.17.2.3 Aufbewahrungsort

Ein weiterer Aspekt der Datensicherung betrifft den Ort, an dem die gesicherten und die archivierten Daten aufbewahrt werden. Dieser sollte zutrittsgeschützt und im Notfall jederzeit zugänglich sein. Zur Optimierung der Lebenserwartung der Datenträger sollte er klimatisiert sowie frei von Rauch, Staub und störenden Magnetfeldern sein.

Es wird zwischen drei Datensicherungsarchiven unterschieden:

- Arbeitsarchiv (in der Nähe des Einsatzorts)
- Sicherheitsarchiv (in einem getrennten Brandabschnitt)
- Katastrophenarchiv (in räumlich hinreichender Entfernung in einem anderen Gebäude).

Bei einer großen Anzahl von Datenträgern sind DV-gestützte Verfahren für deren Verwaltung erforderlich.

9.5.17.2.4 Auslagerungsverfahren

Eine Auslagerungsstrategie definiert, wohin und wie die Daten bzw. Datenträger ausgelagert werden. Dies erfordert organisatorische Regelungen und regelmäßige Tests zum Rückspielen der Daten.

*Auslagerungs-
strategie*

Die Auslagerungsverfahren der Datensicherung unterscheiden sich in

1. zu Fuß („Walk“-Net)
2. netzbasiert, z. B. über LAN, WAN, SAN.

Bei der Auslagerung der Datensicherung zu Fuß transportieren vertrauenswürdige Mitarbeiter die Datenbänder z. B. in eine andere Lokation. Dies erfordert zeitlichen und personellen Aufwand und beinhaltet Transportrisiken, wie z. B. Beschädigung oder Verlust durch Diebstahl. Auch der Rücktransport gestaltet sich aufwändig, da erst jemand zum Aufbewahrungsort fahren, die erforderlichen Bänder herausuchen und abholen muss. Diese Lösung eignet sich daher eher für geringere Sicherheitsanforderungen und für zeitversetzte Datensicherungen.

*Auslagerung zu
Fuß*

Alternativ können die Daten über ein lokales oder Weitverkehrsnetz und mittels gesicherter Übertragung an den Auslagerungsort übertragen und dort gesichert werden. Dies führt zu einer zusätzlichen Belastung des Netzes, sodass die Netzkapazität entsprechend vorhanden sein oder angepasst werden muss. Alternativ kann ein separates Netz, z. B. in Form eines SAN genutzt werden. Dies ermöglicht neben zeitversetzten Datensicherungen auch zeitnahe oder sogar Echtzeit-Datensicherungen. Verfügt das Unternehmen über keinen zweiten Standort, so kann es sich Speicherplatz bei einem Storage Provider anmieten. Hierbei ist auf eine ausreichend verschlüsselte Übertragung und Speicherung zu achten.

*Auslagerung
über LAN oder
WAN*

Bei der netzbasierten Auslagerung erfolgt die Hin- und Rückübertragung schneller, da die Transportzeiten entfallen. Außerdem reduzieren sich die personellen und zeitlichen Aufwände zur Auslagerung und zum Rücktransport.

Verfügt das Unternehmen beispielsweise über zwei Rechenzentren oder zwei Serverräume an unterschiedlichen Lokationen, so kann eine Über-Kreuz-Sicherung erfolgen. Je nach Verfügbarkeitsanforderungen und demgemäßer technischer Auslegung können Bandsicherungen oder Plattenspiegelungen durchgeführt werden. Bei ausreichender räumlicher Trennung kann die Sicherung gleichzeitig als „Online-Katastrophen-Backup“ dienen.

*Über-Kreuz-
Sicherung*

Durch die Über-Kreuz-Sicherung oder Spiegelung in ein ausreichend entferntes und geschütztes Rechenzentrum bzw. bei Servern in einen

entsprechenden Serverraum kann dieses/dieser im Katastrophenfall als Ersatz für das ausgefallene Rechenzentrum bzw. den ausgefallenen Serverraum genutzt werden.

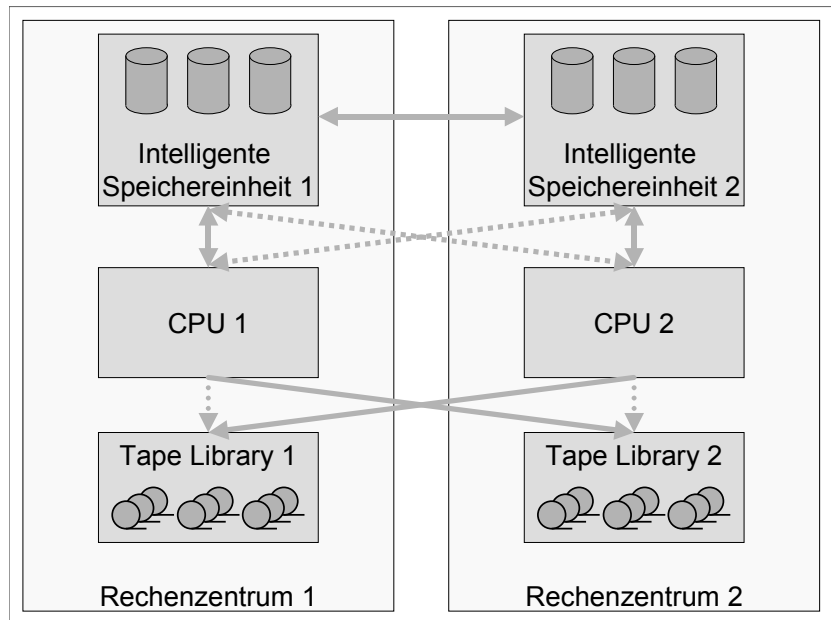


Abb. 9.7: Über-Kreuz-Sicherung

9.5.17.3 Notfall- und Katastrophenvorsorge

*Anforderungen
und Verfügbar-
keitsklassen*

Ausgangspunkt für die angemessene Notfall- und Katastrophenvorsorge sind die Anforderungen der Nutzer. Diese Anforderungen werden zu Verfügbarkeitsklassen gruppiert, für die geeignete und wirtschaftlich vertretbare Sicherheitsmaßnahmen entwickelt werden.

Die Anforderungen ergeben sich zum einen aus unternehmensspezifischen Anforderungen und zum anderen aus gesetzgeberischen, regulatorischen und vergleichbaren Vorgaben, wie sie im Rahmen der Geschäftseinflussanalyse erhoben wurden.



Ordnungsmäßige Buchführung

Das Handelsgesetzbuch (HGB), Stand 5.1.2007, und die Abgabenordnung (AO), Stand 13.12.2006, fordern die Verfügbarkeit der Buchführungsdaten.

Explizit erwartet das HGB gemäß §239, Abs. 4 und §257 Abs. 3, Ziffer 2, dass die Daten „während der Dauer der Aufbewahrungsfrist verfügbar

sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können“.

Die Abgabenordnung (AO) fordert gemäß § 147 Abs. 2, Ziffer 2, dass „die Daten [...] während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können“.

Das Institut der Wirtschaftsprüfer (IDW) verlangt in den „Grundsätzen ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1, 21/2002), (88), „[...] Vorkehrungen für den Notbetrieb [...]“. FAIT 1 führt dort weiter aus: „Ein Ausfall wesentlicher IT-Anwendungen ohne kurzfristige Ausweichmöglichkeit [...] stellt einen wesentlichen Mangel der Buchführung dar.“

Basel II

Die „Sound Practices for the Management and Supervision of Operational Risk“ [34], auf die Basel II [18] verweist, fordern in Prinzip 7: „Banks should have in place contingency and business continuity plans [...]“

Mindestanforderungen an das Risikomanagement (MaRisk)

In den Mindestanforderungen an das Risikomanagement (MaRisk) fordert die BaFin (Rundschreiben 18/2005) ein Notfallkonzept mit Geschäftsfortführungs- und Wiederanlaufplänen. „Die Wirksamkeit [...] des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. [...] Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen.“

Für den Not- oder Katastrophenfall müssen Notfall-Szenarien und die Informations- und Eskalationswege festgelegt werden. Die Mitglieder des Krisenstabs und ihre Stellvertreter, ihre Erreichbarkeit und Entscheidungskompetenz müssen definiert sein. Mitglieder des Krisenstabs sind beispielsweise der verantwortliche Manager sowie die Leiter Sicherheit, Haustechnik, IT, Personal, Finanzen und Öffentlichkeitsarbeit sowie der Vorsitzende des Personal-/Betriebsrats. Darüber hinaus sollten Kompetenzteams definiert sein, die für die Themen Geschäftsprozesse, Haustechnik und Gebäudesicherheit, Telekommunikation und IT zuständig sind. Außerdem sind für den Krisenstab der Raum und der Ersatzraum und seine Ausstattung festzulegen.

*Notfall-
szenarien und
Krisenstab*

Die erforderlichen Aktivitäten sollten unterteilt sein in Sofortmaßnahmen zur Schadensbegrenzung, zur Personalarbeitsbereitschaft und zur Schadensmeldung sowie in mittelfristige Maßnahmen. In Abhängigkeit von der Schadensbewertung trifft der Krisenstab die Entschei-

Maßnahmen

Überblick
über
Ansprech-
partner und
Infrastruktur

dung für oder gegen einen Notbetrieb und beschließt die weiteren Aktivitäten.

Wesentliches Grundelement der Notfallplanung ist der aktuelle Überblick über die internen und externen Ansprechpartner, z. B. ITK, Betriebsschutz, Sicherheitsdienst, Betriebsarzt, Sanitäter, Haustechnik, Versorgungsunternehmen, externe Hilfsorgane wie Feuerwehr und Notarzt, externe Dienstleister, Hersteller und Lieferanten. Eine Übersicht über die vorhandenen Arbeitsplätze und deren Ausstattung sowie die Gebäude- und IT-Infrastruktur ergänzt dieses Grundelement. Für den regulären Betrieb sind Informationen zum Mengengerüst, der Ausfallerträglichkeit, der Personalstärke und den Ansprechpartnern festzulegen. Für den Notbetrieb selbst und für den Übergang zum Notbetrieb müssen die jeweiligen Notfallbeauftragten die diesbezüglichen Minimalanforderungen und Verantwortlichkeiten beschreiben. Außerdem konzipieren sie die Rückkehr zum regulären Betrieb mit den gegebenenfalls erforderlichen Nacharbeiten.

Review, Test,
Schulung,
Übung, Pflege

Die Notfallbeauftragten unterziehen die Notfall- und Katastrophenvorsorgeplanung einem Review und Test. Sie führen Schulungen durch, halten die Pläne aktuell und üben sie mit den Beteiligten.

9.5.17.4 Versicherung

Ein weiteres Element zur Absicherung des Unternehmens besteht darin, Risiken zu verlagern. Hierzu zählt u. a. der Abschluss von Versicherungen, z. B. die Feuer- und die Sachversicherung, die Computer- und Datenmissbrauchsversicherung sowie die Betriebsunterbrechungsversicherung für Fernmelde- und sonstige elektronische Anlagen.

9.5.17.5 Checkliste Kontrollen (Controls)

Einen ersten Überblick über einige wenige aber wesentliche Elemente des Kontinuitätsmanagements verschaffen die Kontrollen der folgenden Tabelle.

Checkliste mit Kontrollen (controls) zum Kontinuitätsmanagement	Zwingend/ Optional	Ja (✓) / Nein (-)
Verfügt das Unternehmen über ein <u>Kontinuitätsmanagement</u> ?	Z	
Gibt es eine <u>Kontinuitätspolitik</u> ?	Z	
Gibt es einen <u>Kontinuitätsmanagementprozess</u> ?	Z	
Berücksichtigt das Kontinuitätsmanagement die primären und sekundären <u>Sicherheitsaspekte</u> , z. B: Integrität, Vertraulichkeit und Verbindlichkeit?	Z	

Checkliste mit Kontrollen (controls) zum Kontinuitätsmanagement	Zwingend/ Optional	Ja (✓) / Nein (-)
Enthält das Kontinuitätsmanagement eine <u>Business Impact Analyse</u> ?	Z	
Enthält das Kontinuitätsmanagement eine <u>Risikoanalyse</u> ?	Z	
Existieren <u>Kontinuitätsrichtlinien</u> bzw. generische Kontinuitätsstandards (Rahmenwerk) mit Prinzipien, Vorgehensweisen und Vorlagen z. B. für Notfall- und Katastrophenvorsorgepläne, Sofortmaßnahmenpläne, Test- und Übungsprotokolle?	Z	
Existieren <u>Übungsportfolio und -plan</u> ?	Z	
...		

9.5.18 Securitymanagement (Security Management)

Das Themenfeld Securitymanagement befasst sich mit dem Schutz vor Angriffen und vor Missbrauch. Es dient der Angriffssicherheit. Wesentliche Elemente dieses Themenfeldes lassen sich durch folgende Modelle veranschaulichen:

- das Sicherheitsschalenmodell des Autors
- das Berechtigungsmodell
- den Berechtigungswürfel bzw. die Berechtigungsmatrix.

Die folgenden Unterkapitel beschreiben diese Modelle. Anschließend erfolgt die Konkretisierung einzelner Elemente des Sicherheitsschalenmodells.

9.5.18.1 Sicherheitsschalenmodell / Sicherheitsschirm

Das Sicherheitsschalenmodell des Autors, auch als Sicherheitsschirm bezeichnet, veranschaulicht den Schutz des Unternehmens, seiner Mitarbeiter, seiner Geschäftsprozesse und der Unternehmenswerte, wie z. B. der Gebäude, der ITK-Systeme und der Infrastruktur, vor Angriffen. Es berücksichtigt die Themenstellungen Schutz von Werten und Schutz vor gefährlichen Ressourcen.

*Sicherheits-
schalenmodell*

Schutz von Werten heißt, dass die Werte, also die Schutzobjekte des Unternehmens, z. B. Gebäude, Räumlichkeiten, Arbeitsplätze, Rechner, Netze, Daten und Personen geschützt werden.

*Schutz von
Werten*

Der Schutz vor gefährlichen Ressourcen beinhaltet, dass sich das Unternehmen vor dem Herein- oder Hinausbringen unerwünschter

*Schutz vor
gefährlichen
Ressourcen*

Ressourcen, wie z. B. Bomben, Gefahrstoffe und Computerviren schützt.

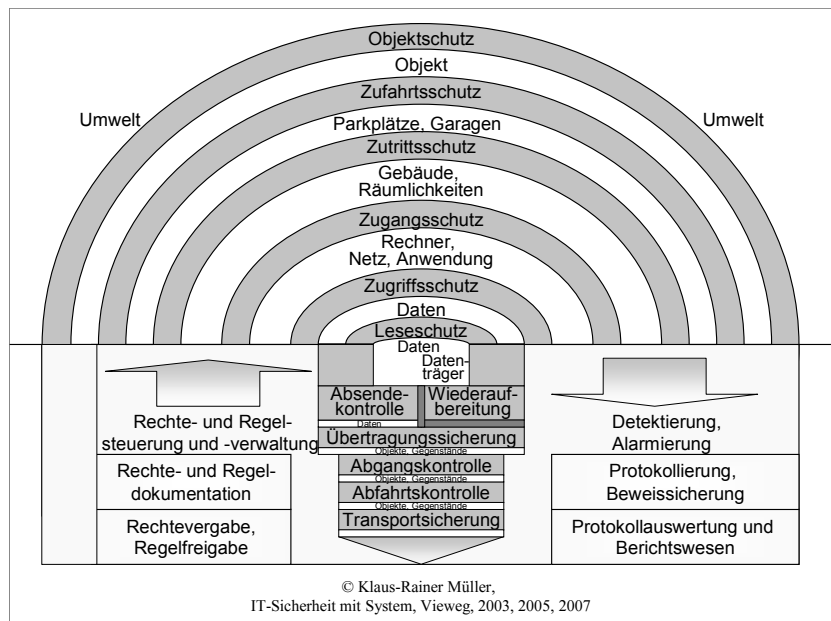


Abb. 9.8: Allgemeines Sicherheitsschalenmodell nach Dr.-Ing. Müller

Schalen als Hürden

Das Sicherheitsschalenmodell stellt die Hürden dar, die ein potenzieller Angreifer, aber auch eine autorisiertes Subjekt, z. B. eine Person, bewältigen müssen, um

- einerseits zu den verschiedenen schutzbedürftigen Werten (Schutzobjekte), bis hin zu den Daten und Informationen zu gelangen oder sie oder Teile davon mitzunehmen und
- andererseits gefährdende Ressourcen in das Unternehmen herein- oder aus ihm hinauszubringen.

Zu berücksichtigen ist hierbei, dass ein Angreifer nicht immer alle Schalen überwinden muss. So vermeidet ein Fußgänger die Schale Zufahrtsschutz und gegen einen Zugang aus dem Internet greift erst die Schale Zugangsschutz.

Stärke der Schalen

Die Sicherheitsschalen können in sich eine unterschiedliche Stärke besitzen, je nachdem, welcher Sicherheitsklasse die zu schützenden Ressourcen angehören. Darüber hinaus kann die Stärke der jeweili-

gen Sicherheitsschale zeitabhängig sein. Bei Terrorwarnungen oder aktuellen Drohungen kann sie beispielsweise hochgesetzt werden und dadurch stärker sein als in ruhigeren Zeiten. So werden Anlieferungen oder Personen in Krisenzeiten oftmals stärker kontrolliert.

Bei der Betrachtung der Schutzwirkung von Sicherheitsmaßnahmen finden Sie häufig den anschaulichen Vergleich mit einer Kette, da eine Kette nur so stark ist wie ihr schwächstes Glied. Wie passt dieser Vergleich zusammen mit den Hürden des Sicherheitsschalenmodells? Da die Wirkung nacheinander zu überwindender Hürden zunimmt, bezieht sich der Vergleich mit einer Kette stets nur auf eine Sicherheitsschale und gleiches Sicherheitsniveau, nicht jedoch quer über alle Hürden hinweg. Wird beispielsweise der Eingang zu einem Gebäude sehr stark geschützt, so wäre dies ein sehr belastbares Glied in der Kette. Gibt es jedoch noch einen weiteren Zutritt zum Gebäude z. B. über eine weniger gesicherte Tür oder gar ungesicherte angeklappte Fenster, so bestimmen diese schwachen Kettenglieder das resultierende Sicherheitsniveau für den Zutritt. Im ITK-Bereich finden sich manchmal stark abgesicherte Netzzugänge, deren Wirkung durch einen „übersehenen“ ungesicherten Netzzugang reduziert wird.

*Schutzwirkung
entspricht
schwächstem
Glied der Kette*

Um den Schutzmechanismus der Sicherheitsschalen zu verwirklichen, ist die Frage zu beantworten, wer wann und mit welchen Rechten an welche schützenswerten Unternehmenswerte gelangen darf. Für die Vergabe von Rechten sind entsprechende Antrags- und Genehmigungsverfahren erforderlich. Darüber hinaus sind teilweise Regeln die Basis für den Schutzmechanismus, z. B. beim Schutz vor Spamming. Diese müssen erstellt und freigegeben sowie gepflegt und weiterentwickelt werden.

Rechtevergabe

Im Hinblick auf die Nachvollziehbarkeit der vergebenen Berechtigungen müssen die genehmigten Anträge für Zufahrts-, Zutritts-, Zugangs-, Zugriffs- und Leserechte dokumentiert und aufbewahrt werden. Dies gilt entsprechend für die oben genannten Regeln.

*Rechte-
dokumentation*

Die Rechtsteuerung und -verwaltung bildet die genehmigten Berechtigungen ab (administriert sie). Sie steuert beispielsweise, wer welche Daten lesen und wer sie auch verändern darf. Dies gilt entsprechend für die Verwaltung der Regeln und die daraus resultierende Steuerung.

*Rechte-
steuerung und
-verwaltung*

Die äußerste Sicherheitsschale bildet der Objektschutz, der das Gebäude vor der Umwelt schützt. Er teilt sich auf in äußeren und inneren Objektschutz.

Objektschutz

<i>Äußerer Objektschutz</i>	Der äußere Objektschutz sichert das Gelände und das Gebäude nach außen hin. Zu ihm gehören beispielsweise Zäune, die Außenhautüberwachung mittels Kameras und das Wachpersonal, das Streife geht.
<i>Innerer Objektschutz</i>	Der innere Objektschutz schützt die Infrastruktur des Gebäudes. Er beinhaltet z. B. eine Einbruchmeldeanlage (EMA), auf die Sensoren an den Fensterscheiben hindeuten.
<i>Zufahrtsschutz</i>	Die Zufahrt zum Gebäude sichert eine weitere Schale. Zufahrt erhalten dabei nur Fahrzeuge und Personen, welche die Sicherheitsanforderungen erfüllen.
<i>Zutrittsschutz</i>	Den Zutritt zum eigentlichen Gebäude sichert die nächste Schale des Schalenmodells in Form des Zutrittsschutzes. Als Zutrittskontrollsystem (ZKS) finden sich häufig Türen oder Drehkreuze mit Leseinheiten für Magnet- oder Chipkarte. Darüber hinaus befindet sich am Eingang üblicherweise ein Empfang für Besucher. Die sicherheitsrelevanten Räumlichkeiten, wie z. B. Rechenzentren, Wertpapier-Handelsräume und Technikräume (Kommunikationstechnik, Etagenverteiler, Serverräume etc.) sichern Unternehmen durch stärkere Zutrittskontrollsysteme, im Fall des Rechenzentrums z. B. durch Personen-Vereinzelungsanlagen. Auch Vorstandsbereiche verfügen meist über zusätzliche Schutzmaßnahmen.
<i>Zugangsschutz</i>	Der Zugangsschutz bildet die folgende Schale. Er sichert den Zugang zu Informationssystemen und den unternehmenseigenen Netzen, indem sich Benutzer identifizieren und authentisieren müssen. Dies erfolgt oftmals durch die Benutzerkennung (UserId) und das Passwort. Darüber hinaus schützen Firewalls sowie Intrusion-Detection- und -Response-Systeme den Zugang zum unternehmenseigenen Netz.
<i>Zugriffsschutz</i>	Die fünfte Schale besteht aus dem Zugriffsschutz. Er bestimmt den Zugriff auf Ressourcen, wie z. B. Daten, Dateien, Datenbanken, Transaktionen und Anwendungsteile. Zugriffsrechte erhalten jene Personen, welche den Zugriff auf die jeweiligen Daten zur Aufgabenerfüllung benötigen. Den Zugriff auf Personaldaten erhält beispielsweise nur die Personalabteilung und der jeweils zuständige Vorgesetzte. Zugriffsschutz gibt es daneben auch für papierhafte Dokumente, indem diese in entsprechende Vertraulichkeitsklassen bzw. Geheimhaltungsstufen eingeteilt sind. Hier erfolgt der Zugriffsschutz über organisatorische Regelungen und die sichere Verwahrung z. B. in Safes.

Eine weitere Schale bildet der Leseschutz. Er macht Daten z. B. durch Verschlüsselung nur für Berechtigte lesbar. *Leseschutz*

Da sich Daten situativ auf unterschiedlichen Medien befinden, z. B. im Hauptspeicher, auf Festplatten, auf Disketten oder Bändern, ist neben dem Zugriffs- und Leseschutz ein weiteres Schutzelement erforderlich. Dieses Schutzelement, die Wiederaufbereitung [14], soll sicherstellen, dass Speichermedien vor ihrer anderweitigen Verwendung so gelöscht sind, dass keine Rückschlüsse auf ihren ursprünglichen Inhalt möglich sind. *Wiederaufbereitung*

Bis hierher hat ein Subjekt den Weg über die verschiedenen Schalen und Objekte bis zu den Daten und dem Datenträger zurückgelegt. Nun gilt es, den Weg abzusichern, den die Objekte, z. B. die Daten, nehmen, wenn sie sich von ihrem „regulären“ und geschützten Ort entfernen.

Hierbei ist zuerst zu prüfen, ob die Daten die z. B. über ein WAN weitergeleitet werden sollen, versendet werden dürfen. Hierzu dient die Absendekontrolle. Beispielsweise dürfen geheime Daten das Unternehmen nicht oder nur verschlüsselt verlassen, oder Spam-Mails sowie E-Mails mit Viren nicht versandt werden. *Absendekontrolle*

Damit die Zugriffsberechtigten mit den Daten arbeiten können, müssen diese vom Aufbewahrungsort, dem Großrechner oder Server über das Netz (LAN, WLAN, WAN, MAN, Internet) zum Terminal, thin client oder PC transportiert werden. Während der Übertragung müssen die Daten bzw. Informationen der jeweiligen Sicherheitsstufe entsprechend geschützt sein. Zum Schutz der Übertragung dient die Übertragungssicherung. *Übertragungssicherung*

Werden Daten z. B. auf Datenträgern oder auf Papier aus dem Unternehmen hinaus transportiert, so ist sicherzustellen, dass diese Daten das Unternehmen verlassen dürfen. Dies gilt auch für physisches Eigentum des Unternehmens und für Gefahrstoffe. Um dies zu erreichen, gibt es die Abgangskontrolle. *Abgangskontrolle*

Ein weiteres Kontrollelement ist die Abfahrtskontrolle. Sie soll erreichen, dass kein Eigentum oder gefährliche Objekte das Unternehmen unzulässigerweise verlassen. *Abfahrtskontrolle*

Werden z. B. papierhafte Dokumente oder Datenträger zum Auslagerungsort gebracht, so muss der Transport in gesicherter Form erfolgen, beispielsweise verschlüsselt und/oder in gesicherten Behältnissen sowie durch eine sichere Transportorganisation. Hierzu dient die Transportsicherung. *Transportsicherung*

*Alarmierung,
Protokollierung
und Beweis-
sicherung*

*Protokoll-
auswertung,
Berichtswesen*

Um die Schutzwirkung der Sicherheitsschalen verfolgen und später auswerten zu können, müssen die verschiedenen Schutzsysteme sicherheitsrelevante Ereignisse protokollieren können und bei Sicherheitsverletzungen alarmieren.

Die Systemadministratoren müssen die Protokolle zeitnah auswerten, um sicherheitsrelevante Vorfälle frühzeitig zu erkennen. Regelmäßige Berichte fassen die Ergebnisse zusammen.

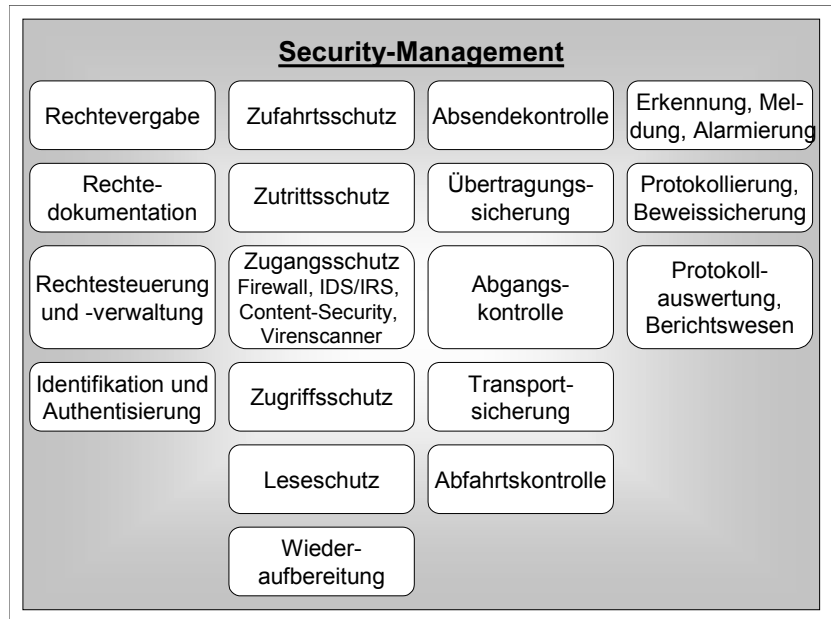


Abb. 9.9: Elemente des Securitymanagements gemäß Sicherheitsschalenmodell nach Dr.-Ing. Müller

*Elemente der
Security-
Architektur*

Insgesamt ergeben sich aus dem Sicherheitsschalenmodell folgende Elemente der Security-Architektur:

- Rechtevergabe
- Rechedokumentation
- Rechtesteuerung und -verwaltung
- Objektschutz
- Zufahrtsschutz
- Zutrittsschutz
- Zugangsschutz
- Zugriffsschutz
- Leseschutz

- Wiederaufbereitung
- Absendekontrolle
- Übertragungssicherung
- Abgangskontrolle
- Transportsicherung
- Abfahrtskontrolle
- Alarmierung, Meldung
- Protokollierung/Beweissicherung
- Protokollauswertung und Berichtswesen.

Die Abbildung stellt diese Elemente des Securitymanagements, zu denen unternehmensspezifische Verfahren, Tools und Hilfsmittel festzulegen sind, dar. Die folgenden Unterkapitel beschreiben diese Elemente des Sicherheitsschalenmodells näher.

9.5.18.2 Berechtigungsmodell

Für die verschiedenen Schalen des Sicherheitsschalenmodells muss definiert werden, wer diese Schalen passieren darf und wer abgewiesen wird. Dies erfordert zur Umsetzung einen Steuerungsmechanismus, der auf der Rechteverwaltung basiert.

*Rechte-
steuerung und
-verwaltung*

Gemeinsames Grundprinzip für den Zufahrts-, Zutritts-, Zugangs- und Zugriffsschutz ist es, dass ein Subjekt (z. B. eine Person) für ein Objekt (z. B. Gebäude, Räume, Anwendungen, Daten) bestimmte Rechte erhält.

Beim Zufahrtsschutz erhalten bestimmte Subjekte, wie z. B. Personen oder Lieferfirmen, das Recht, das Gelände zu bestimmten Zeiten in bestimmten Bereichen zu befahren.

Zufahrtsschutz

Beim Zutrittsschutz erhalten bestimmte Personen das Recht, zu bestimmten Zeiten Zutritt zu bestimmten Gebäuden oder Räumlichkeiten zu erhalten.

Zutrittsschutz

Beim Zugangsschutz erhalten Subjekte, z. B. Personen, das Recht, bestimmte Objekte, z. B. Rechner, Netz oder Anwendungen (zu bestimmten Zeiten) zu nutzen.

Zugangsschutz

Durch den Zugriffsschutz erhalten Subjekte, wie z. B. Personen oder Anwendungen, spezielle Rechte (z. B. lesen, anlegen, ändern, schreiben, löschen) auf Objekte, wie z. B. Daten.

Zugriffsschutz

Der Berechtigungswürfel (Berechtigungskubus) des Autors kann für jede der vier Sicherheitsschalen Zufahrts-, Zutritts-, Zugangs- und Zugriffsschutz genutzt werden. Er veranschaulicht die Kombination aus Subjekt, Recht und Objekt.

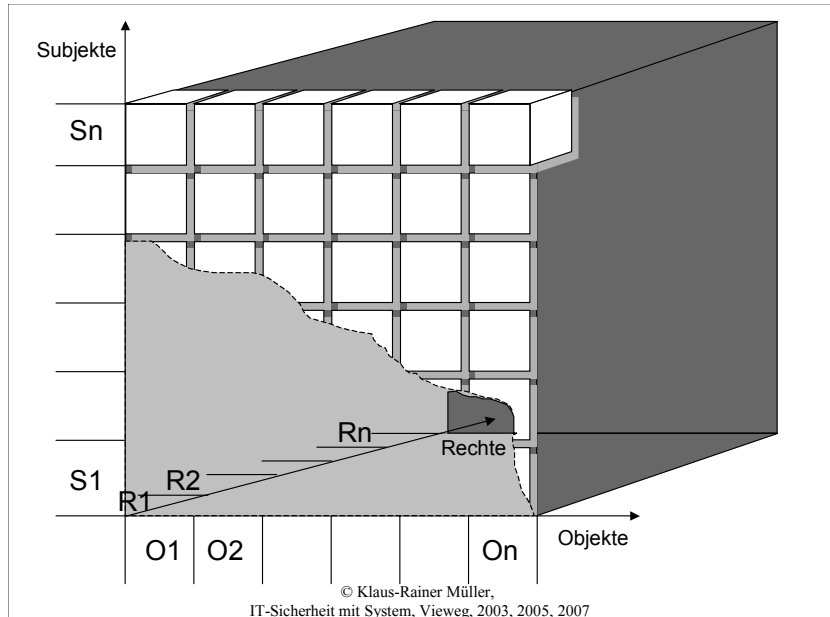


Abb. 9.10: Berechtigungswürfel bzw. -kubus

Drei
Dimensionen:
Subjekt, Recht,
Objekt

Die x-Koordinate des Berechtigungswürfels repräsentiert jene Objekte (oder Objektgruppen), für die ein Recht erteilt werden soll. Auf der y-Koordinate sind die Subjekte (oder Subjektgruppen {Rollen}) eingetragen, die ein Recht erhalten sollen. Die Art des Rechts wird in z-Richtung angegeben. Es entstehen einzelne Würfel, welche die jeweilige Subjekt-Recht-Objekt-Kombination wiedergeben. Die jeweils erteilten Zugriffsberechtigungen in Form einer Subjekt-Recht-Objekt-Beziehung können farblich herausgehoben werden.

Die dreidimensionale Darstellung lässt sich in eine zweidimensionale transformieren, indem statt des jeweiligen Subjekt-Objekt-Würfels ein Subjekt-Objekt-Feld verwendet wird, in dem die dazugehörigen Rechte aufgelistet werden.

Berechtigungs-
würfel bzw.
-kubus

Berechtigungs-
vergabe und
-pflege

Die individuelle Vergabe und Pflege dieser Berechtigungen wird mit zunehmender Zahl der Subjekte und Objekte komplexer. Bei einem Unternehmen mit 1.000 Mitarbeitern (Subjekte) und 100 Ressourcen (Objekte), zu denen die Mitarbeiter unterschiedliche Rechte erhalten, ergeben sich je nach Anzahl der Rechte einige 100.000 mögliche Subjekt-Recht-Objekt-Kombinationen. Es lässt sich leicht nachvollziehen, dass ein solches Berechtigungsgebilde schwer überschaubar und

kaum mehr handhabbar, geschweige denn kontrollierbar wäre. Wie kann diese Komplexität reduziert werden?

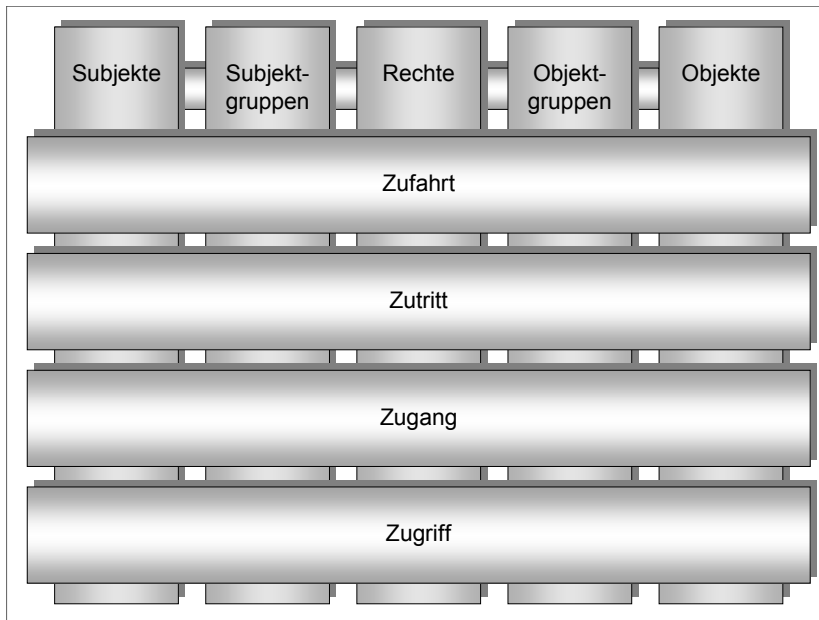


Abb. 9.11: Subjekt-Subjektgruppe-Recht-Objektgruppe-Objekt-Modell

Hierzu muss die Organisationsstruktur des Unternehmens näher betrachtet werden. Insbesondere in größeren Unternehmen nehmen verschiedene Subjekte (z. B. Personen) regulär oder als Stellvertreter die gleichen Aufgaben (Rolle) wahr bzw. haben die gleiche Zuständigkeit. Diese benötigen zur Durchführung ihrer Aufgaben somit die gleichen Rechte auf bestimmte Objekte.

*Komplexitäts-
reduktion*

Zur Vereinfachung und Effizienzsteigerung bei der Administration sowie zur Steigerung der Transparenz werden daher Subjektgruppen gebildet. Einer solchen Gruppe werden die Subjekte, welche die gleichen Rechte erhalten sollen, zugeordnet. Hierdurch lässt sich die Administration vereinfachen. Neue Mitarbeiter, oder Mitarbeiter, die eine neue Aufgabe wahrnehmen, müssen dann nur noch den jeweiligen Subjektgruppen zugeordnet und gegebenenfalls aus vorherigen Subjektgruppen gelöscht werden. Hierdurch lässt sich neben dem Aufwand auch die Fehleranfälligkeit gegenüber dem individuellen Anlegen von Berechtigungsprofilen verringern.

Subjektgruppen

<i>Objektgruppen</i>	Analog wird bei Objekten verfahren. Beispielsweise lassen sich mehrere Drucker, alle Dateien eines Verzeichnisses oder Dateien mit gleichem Zugriffsprofil zu Objektgruppen zusammenfassen. Die Bildung von Gruppen für Subjekte und Objekte sowie deren Verknüpfung mit Rechten lässt sich mittels des abgebildeten Subjekt – Subjektgruppe – Recht – Objektgruppe – Objekt – Modells veranschaulichen.
<i>Gruppenbildung</i>	Entscheidend für die Effizienz und Transparenz ist die geeignete Gruppenbildung. Diese leitet sich bei Personen einerseits von ihren Aufgaben bzw. Rollen im Unternehmen und andererseits von der Zugehörigkeit zu einer Organisationseinheit ab. Gleichzeitig ist das „Prinzip der minimalen Rechte“ zu beachten. D. h. jedes Subjekt erhält nur die Rechte auf jene Objekte, die es für die Ausübung seiner Aufgaben mindestens benötigt.

9.5.18.3 Rechtevergabe

Für die Vergabe von Rechten muss der Sicherheitsbeauftragte ein entsprechendes Antrags- und Genehmigungsverfahren festlegen. Für die schützenswerten Ressourcen, wie z. B. Anwendungen und Daten, definieren die Ressourcenverantwortlichen, welche Teilobjekte es gibt und mit welchen Rechten auf diese zugegriffen werden kann. Für jede Anwendung und deren Daten werden Eigentümer und Stellvertreter festgelegt, die für die Definition der Rollen und die Genehmigung der Anträge verantwortlich sind.

9.5.18.4 Rechtedokumentation

Die vergebenen, veränderten oder zurückgenommenen Berechtigungen müssen in nachvollziehbarer Form revisionssicher dokumentiert und archiviert werden. Hierdurch muss jederzeit eindeutig ermittelt werden können, welches Subjekt wann welche Rechte auf welche Objekte besessen hat.

9.5.18.5 Rechtsteuerung und -verwaltung

Die Rechtsteuerung und -verwaltung und damit die Freischaltung oder Sperrung einer Sicherheitsschale erfolgt über entsprechende Systeme, in denen die vergebenen Rechte hinterlegt sind. So wird Ihnen beispielsweise bei Nutzung Ihrer unternehmensspezifischen Chipkarte vom dahinter liegenden Rechtsteuerungs- und -verwaltungssystem Zufahrt zur Garage oder Zutritt zum Gebäude gewährt. Die Administration der Rechteverwaltungssysteme kann zentral oder dezentral erfolgen.

Die Rechtsteuerungs- und -verwaltungssysteme der verschiedenen Betriebssysteme sind in der Regel unterschiedlich. Dies macht jeweils spezielle Kenntnisse der Administratoren erforderlich. Bei sehr umfangreicher und heterogener Systemlandschaft setzen IT-Bereiche hier bei Bedarf übergeordnete Rechteverwaltungssysteme ein, die eine zentrale und einheitliche Steuerung und Administration ermöglichen („Single Point of Security Control and Administration“, SPSCA).

*Rechte-
steuerungs-
und
-verwaltungs-
system*

9.5.18.6 Objektschutz

Der Objektschutz unterteilt sich in den äußeren und inneren Objektschutz. Zum äußeren Objektschutz gehört die Absicherung und Überwachung des Areals, auf dem sich das oder die Gebäude befinden, sowie des Umfelds, damit Gefahren frühzeitig erkannt werden können. Auch innerhalb von Gebäuden existiert im Umfeld sicherheitskritischer Bereiche oftmals eine Videoüberwachung, quasi als innerer Perimeterschutz. Darüber hinaus schützen innerhalb des Objektes Gefahrenmeldeanlagen bestehend aus Einbruch-, Brand- und Wassermeldeanlage das Objekt und seine Werte.

9.5.18.7 Identifikation und Authentisierung

Beim Zufahrts-, Zutritts-, Zugangs- und Zugriffsschutz kommt das Verfahren der Identifikation und – insbesondere beim Zugangsschutz – der Authentisierung zum Einsatz. Das Subjekt, z. B. ein Benutzer, identifiziert sich über seine Benutzerkennung. Um zu überprüfen, ob die Identität des Benutzers mit der verwendeten Benutzerkennung übereinstimmt, muss sich der Benutzer zusätzlich authentisieren.

9.5.18.7.1 Identifikation

Jeder Benutzer erhält eine eindeutige, d. h. umkehrbar eindeutige Benutzerkennung. Das bedeutet, dass das Computersystem nach der Anmeldung nicht nur dem Nutzer eindeutig ein Benutzerkonto zuweist, sondern dass umgekehrt die Nutzung des Benutzerkontos auch eindeutig einem Benutzer zugeordnet werden kann.

Werden also beispielsweise unter einem Benutzerkonto Aktivitäten entfaltet, so können diese dem entsprechenden Benutzer eindeutig zugeordnet werden. Eine Mehrfachnutzung ein und desselben Benutzerkontos durch verschiedene Benutzer ist hierbei verboten. Auf diesem Wege ist die prinzipielle Rückverfolgbarkeit der Aktivitäten gegeben.

Für die Bildung der Benutzererkennung sollte ein unternehmensweit einheitliches Schema in Form einer Namenskonvention verwendet werden.

9.5.18.7.2 Authentisierungsarten

Die Authentisierung ist auf unterschiedlichen Wegen möglich. Folgende Authentisierungsarten werden unterschieden:

- Authentisierung durch Wissen
- Authentisierung durch Besitz
- Authentisierung durch Merkmal
- Authentisierung durch Verhalten.

Darüber hinaus gibt es Kombinationen aus den Basis-Authentisierungsarten, z. B.

- Authentisierung durch Wissen und Besitz
- Authentisierung durch Merkmal bzw. Verhalten und Wissen
- Authentisierung durch Besitz und Merkmal bzw. Verhalten.

Soviel zur Theorie. Doch wie stellen sich diese Authentisierungsarten in der Praxis dar? Die folgenden Beispiele veranschaulichen dies:

Authentisierung durch Wissen

- Authentisierung durch Wissen
Authentisierung durch Wissen ist eine weit verbreitete Authentisierungsart. Sie finden sie z. B. in Form des Passworts, das Sie beim Anmelden an ein Computersystem eingeben oder auch in Form der PIN (Personal Identification Number) bei Scheckkarten.

Authentisierung durch Besitz

- Authentisierung durch Besitz
Authentisierung durch Besitz eines Gegenstandes finden Sie beispielsweise in Form eines Schlüssels, eines Ausweises, einer Chipkarte oder eines USB-Tokens.

Authentisierung durch Merkmal

- Authentisierung durch Merkmal
Persönliche (biometrische) Merkmale, die sich zur Authentisierung nutzen lassen, reichen vom Fingerabdruck, dem Regenbogenhaut- (Iris-), Netzhaut- (Retina-), Handlinien-, Handvenen- und Stimmenmuster, der Hand-, Zweifinger-, Ohr-, Kopf- und Gesichtsgeometrie über das thermische Gesichtsbild sowie das Aussehen (Foto) bis hin zur menschlichen DNA (genetischer Fingerabdruck). Authentisierung durch geeignete persönliche Merkmale gelangt insbesondere bei Zutritts-, aber auch Zugangskontrollsystemen zum Einsatz.

- **Authentisierung durch Verhalten**
Ein altbekanntes Verfahren, persönliches Verhalten zur Authentisierung zu nutzen, ist die Unterschrift. Weitere Verhaltensmuster ergeben sich aus der Sprechweise, den Lippenbewegungen, dem Gang und dem Tippverhalten an einer Tastatur. *Authentisierung durch Verhalten*
- **Authentisierung durch Wissen und Besitz**
Authentisierung durch Wissen und Besitz ist zum Beispiel bei Scheckkarten oder Kreditkarten gegeben. Der Besitz ist in diesem Fall die Karte, das Wissen die PIN. *Authentisierung durch Wissen und Besitz*
- **Authentisierung durch Merkmal und Wissen**
Persönliches Merkmal ist beispielsweise der Fingerabdruck. Zusätzlich muss aber Wissen genutzt werden, z. B. eine PIN (Personal Identification Number) bekannt sein und eingegeben werden. *Authentisierung durch Merkmal und Wissen*
- **Authentisierung durch Besitz und Merkmal**
Ein Beispiel hierfür ist der Zutrittsschutz zu sicherheitsrelevanten Räumlichkeiten. Nach Identifikation mittels der Zutrittskarte erscheint das Bild des Inhabers auf dem Bildschirm und kann entweder automatisch oder durch Wachpersonal überprüft werden, bevor der Zutritt gewährt wird. *Authentisierung durch Besitz und Merkmal*

Biometrie

Bei der Sicherheitsbewertung von biometrischen Verfahren spielen die False Acceptance Rate (FAR) und die False Rejection Rate (FRR) sowie die Überlistungsmöglichkeiten eine wesentliche Rolle. FAR und FRR kennzeichnen, wie oft statistisch ein Objekt fälschlicherweise akzeptiert oder abgelehnt wird.

Ein weiterer sicherheitsrelevanter Faktor ist die „Intelligenz“ und Lebenderkennung der eingesetzten Geräte, die sich u. a. nicht durch ein Foto, Tonband- oder Videoaufnahmen sowie Nachbildungen, wie z. B. künstliche Gesichtsnachbildungen (Masken) oder künstliche Fingerabdrücke, überlisten lassen dürfen.



Ein häufiger Anwendungsfall ist die Authentisierung mittels Passwort. Hierbei ist die Stärke des Passworts von entscheidender Bedeutung. Untersuchungen (z. B. BBC News: Warning over password security, 24. Juni 2002) über die verwendeten Passwörter zeigen oftmals leicht ermittelbare Passwörter, die Sicherheitslücken darstellen. Ein extremes Beispiel ist das Betätigen der „RETURN“-Taste ohne Eingabe eines Passworts. Weitere Beispiele sind die Nutzung des eigenen Vor- oder Nachnamens, des Namens eines Kindes oder Partners oder lexikalisch ermittelbarer Wörter als Passwort.

Authentisierung mit Passwort

Knacken von Passwörtern

Für die Ermittlung von Passwörtern können unterschiedliche Methoden verwendet werden. Ihre Kenntnis hilft, entsprechende Gegenmaßnahmen im Hinblick auf Passwortge- und -verbote zu treffen. Zu diesen Methoden gehört:

- das Erraten von Passwörtern (password guessing) anhand üblicher Kombinationen von Benutzerkennung und Passwort, z. B. Admin/Admin, Gast/Gast oder im System vorinstallierter Benutzerkennungen und zugehöriger Passwörter. Zu derartigen Systemen gehören u. a. Computersysteme, Anwendungen, TK-Anlagen
- das systematische Probieren von Passwörtern (password cracking). Hierbei werden z. B. Wörter aus Wörterbüchern als Passwort genutzt und anschließend nach dem gleichen Algorithmus, den das zugrundeliegende Betriebssystem nutzt, verschlüsselt. Das Ergebnis wird mit den Einträgen in der zuvor gestohlenen Passwortdatei verglichen. Anstelle der Wörter können in der Folge systematisch Kombinationen des kompletten Zeichensatzes durchprobiert werden
- die Ermittlung von Passwörtern über das soziale Umfeld (social hacking), z. B. des Geburtstags oder des Spitznamens.

Darüber hinaus besteht die Möglichkeit, die Eingabe oder Übertragung von Passwörtern mitzuhören oder abzufangen und für Angriffe zu verwenden.

Hinweise für Passwörter

Aufgrund der genannten Angriffsmethoden benötigen Anwender Hinweise einerseits auf unsichere Passwörter und andererseits für die Bildung geeigneter Passwörter und den Umgang damit. Wie die Erfahrung zeigt, ist auch dies nicht ausreichend. Notwendig ist daher die zusätzliche Prüfung durch den Computer, dass die Vorgaben zur Passwortbildung eingehalten worden sind.



Abb. 9.12: USB-Token (Prinzipdarstellung)

Eine Möglichkeit zum Logon durch Wissen und Besitz stellt die Nutzung entsprechender USB-Tokens dar. Zum Einloggen benötigt der Nutzer das Passwort und den USB-Token, den er in die USB-Schnittstelle des Computers einsteckt. Je nach Ausstattung derartiger USB-Tokens können Funktionalitäten integriert sein, die den Computer beim Abziehen des Tokens sperren, die Festplattenverschlüsselung unterstützen, das Signieren von Transaktionen und Dokumenten mittels integrierter PKI-Technologie ermöglichen und Näherungstechnologie für den Gebäudezutritt enthalten.

Authentisierung durch Wissen und Besitz

Eine spezielle Variante der Authentisierung mittels Passwort sind Einmal-Passwörter (One Time Password {OTP}). Durch deren nur einmalige Verwendung kann die Sicherheit erhöht werden. Ein bekanntes Konzept, Einmal-Passwörter zu realisieren, besteht in der Nutzung eines Taschenauthentifikators, der auch Token genannt wird.

Einmal-Passwörter

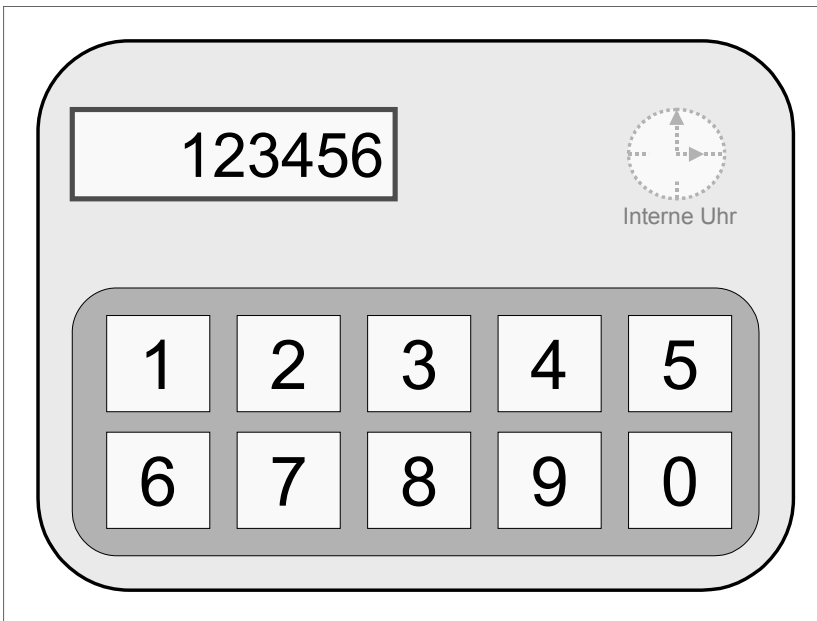


Abb. 9.13: Taschenauthentifikator (Prinzipdarstellung)

Eine Form des Tokens besitzt eine Anzeige, ein Eingabefeld, eine interne Uhr und einen geheimen Schlüssel. Der Benutzer gibt seine PIN in den Token ein. Dieser kombiniert daraufhin die PIN mit dem geheimen Schlüssel und der Uhrzeit zu einem Passwort und zeigt es an. Der Benutzer gibt dieses Passwort ein. Der Host überprüft das

Taschenauthentifikator, Token

ankommende Passwort, indem er mit seiner eigenen Uhr und einer Kopie des geheimen Schlüssels das erwartete Ergebnis berechnet. Stimmen beide überein, so ist die Authentifizierung erfolgreich.

In der Praxis können Gangunterschiede zwischen der internen Uhr des Tokens und der des Host zu Abweichungen führen. Um dies zu vermeiden, berechnet der Host die erwarteten Ergebnisse für ein bestimmtes Zeitfenster. Damit das Zeitfenster möglichst klein bleibt, kann der Host den aktuellen Gangfehler des Tokens in einer Datenbank mitführen und bei jedem Anmeldevorgang aktualisieren. Da eine Wiederverwendung des Passworts innerhalb des Zeitfensters möglich ist, sollte sich der Host bereits vergebene Passwörter merken, deren Wiederverwendung ablehnen, melden und protokollieren.

*Challenge-
Response-
Verfahren*

Ein anderes Verfahren, das Einmal-Passwörter nutzt, ist das Challenge-Response-Verfahren mit Token [35]. Der Token verfügt über ein Eingabefeld, eine Anzeige und einen geheimen Schlüssel. Nach Anwahl durch den Client-PC sendet der Host eine Challenge. Der Benutzer aktiviert den Token mit seiner persönlichen PIN und gibt die Challenge ein. Der Token kombiniert die Challenge mit dem geheimen Schlüssel und zeigt die Response an. Der Benutzer gibt die Response am Client ein, der diese an den Host sendet. Stimmt die übermittelte Response mit der vom Host erwarteten überein, so ist die Authentifizierung erfolgreich. Das Challenge-Response-Verfahren vermeidet die Gangfehler-Problematik, ist aber für den Nutzer aufwändig und tippfehleranfällig.

9.5.18.7.3 Single Sign-on

*Passwort-
Vielfalt beim
Zugangsschutz*

Werden in einem Unternehmen eine Vielzahl von Anwendungen genutzt, so muss sich der Benutzer oftmals viele unterschiedliche Passwörter, teilweise sogar unterschiedliche Benutzerkennungen, merken. Hinzu kommt, dass die Bildungsregeln und Wechselintervalle der Passwörter in den Anwendungen unterschiedlich sind, weil z. B. Passwortrichtlinien fehlen und nicht in den Lebenszyklus des Systems integriert sind. Dies führt dazu, dass Benutzer Passwörter öfter vergessen, dementsprechend häufiger beim Help Desk anrufen und so die Help-Desk-Kosten in die Höhe treiben, oder sich dazu verleiten lassen, Passwörter zu notieren.

*Passwort-
Vielfalt beim
Zutrittschutz*

Dasselbe gilt auch für den Zutrittschutz. Erinnern Sie sich noch an Hausmeister und Haustechniker, die mit einem riesigen Schlüsselbund herumlaufen? Heutzutage wird der Zutritt meist elektronisch geregelt, aber auch hier gibt es in Unternehmen oftmals unterschiedliche Zutrittskontrollsysteme mit verschiedenen Passwörtern und unterschiedlichen Wechselintervallen.

Um diesen Schwierigkeiten entgegen zu wirken, kann das Single Sign-on verwendet werden. Hier genügt ein einmaliges Sign-on, beispielsweise mittels einer Chipkarte zusammen mit einem Passwort oder einem biometrischen Authentisierungsverfahren, um sich bei allen Zugangskontrollsystemen zu identifizieren und zu authentisieren. Der Vorteil dieser Vereinfachung für den Nutzer geht einher mit höheren Anforderungen an die Verfügbarkeit, Vertraulichkeit und Skalierbarkeit des eingesetzten Single-Sign-on-Systems. Das Single-Sign-on-Verfahren kann entsprechend auch für die Zutrittskontrolle eingesetzt werden, um den Zutritt zu allen geschützten Gebäuden und Räumlichkeiten zu steuern.

Lösung:
Single
Sign-on

Es gibt folgende Arten von Single-Sign-on-Systemen:

1. Passwortsynchronisierende Systeme
2. Ticket-basierte Systeme
3. Zwischengeschaltete Single-Sign-on-Systeme
4. Föderierte Systeme (Föderiertes Identitätsmanagement)

Bei Passwort-Synchronisationssystemen meldet sich der Benutzer nur bei diesem System an. In der Folge übernimmt das Passwort-Synchronisationssystem die Anmeldung bei anderen Systemen und Anwendungen einschließlich der Verwaltung der dazugehörigen Benutzerkennungen und Passwörter sowie bei letzteren auch deren Änderungen. Eine Sicherheitslücke kann hierbei entstehen, wenn Passwörter unverschlüsselt über das Netz übertragen werden.

Passwort-
synchronisie-
rende Systeme

Ticket-basierte Systeme vergeben „Tickets“, mit denen sich das Programm auf dem PC des Benutzers gegenüber anderen Anwendungen ausweist. Kerberos™ (s. a. [36], [37]) beispielsweise, das vom MIT (Massachusetts Institute of Technology) entwickelt wurde, arbeitet mit zwei Tickets. Der Benutzer meldet sich über seinen PC (Client) beim KDC (Key Distribution Center) an. Der Authentication Server (AS) im KDC übermittelt dem Client ein TGT (Ticket Granting Ticket). Möchte der Benutzer in der Folge Ressourcen, z. B. Anwendungen, nutzen, so weist sich der Client gegenüber dem KDC mit dem TGT aus und fordert den gewünschten Dienst an. Das TGS (Ticket Granting System) im KDC übermittelt ein Service-Ticket, das zur Nutzung des gewünschten Dienstes berechtigt. Der Client weist sich gegenüber dem angeforderten Dienst mit dem Service-Ticket aus und erhält Zugang. Zur Implementierung von Kerberos™ müssen die bestehenden Systeme entsprechend angepasst werden.

Ticket-basierte
Systeme



Schwachstellen in MIT Kerberos™ 5

Am 3. September 2004 meldete das US-CERT unter der Bezeichnung TA04-247A mehrere Schwachstellen in der MIT-Kerberos™-5-Implementierung.

*Zwischengeschaltete
Single-Sign-on-
Systeme*

Zwischengeschaltete Single-Sign-on-Systeme befinden sich als Middleware zwischen dem primären Authentifizierungssystem und der Anwendung. Hierbei lassen sich zentrale und dezentrale Systeme unterscheiden. Während die benötigten Informationen bei dezentralen Systemen auf der Chipkarte oder dem Token des Benutzers abgelegt sind, verfügen zentrale Systeme über einen Server, der die Benutzer- und Rechteverwaltung durchführt und die Einhaltung der Passwort-Regeln steuert. Zentrale Systeme bieten darüber hinaus die Möglichkeit, die Anmeldevorgänge zentral zu auditieren und Systemzugänge zentral zu sperren. Zentrale Systeme müssen jedoch ausfallsicher gestaltet sein, um einen „Single Point of Failure“ zu vermeiden.

*Föderiertes
Single Sign-on,
föderiertes
Identitäts-
management*

Nutzer web-basierter Online-Services personalisieren diese oftmals. Sie verfügen bei unterschiedlichen Providern meist über unterschiedliche Benutzernamen und Passwörter. Jeder dieser Provider speichert entsprechende Nutzerprofile, in denen neben Benutzername und Passwort gegebenenfalls persönliche Daten, personalisierte Informationen und Präferenzen des Nutzers abgelegt sind. Was bedeutet das für den Benutzer?

Er muss sich entsprechend der Anzahl der Provider verschiedene unterschiedliche Benutzernamen und Passwörter merken. Bei den Providern gespeicherte persönliche Daten, wie z. B. Adressen und Telefonnummern, muss der Benutzer im Falle der Änderung bei jedem dieser Provider pflegen und bei neuen Providern komplett neu eingeben. Wäre es nicht besser, der Benutzer hätte bei den von ihm gewählten Providern die Möglichkeit zum Single Sign-on und zur durchgängigen quasi automatischen Aktualisierung seiner dortigen Daten nach einer Änderung?

Gleichzeitig sind Provider in einem föderierten Geschäftsmodell daran interessiert, ihren Kunden gemeinsame sich ergänzende Dienstleistungen anzubieten. Sie möchten dabei vertrauenswürdige Informationen über die Identität des jeweiligen Kunden erlangen und idealerweise auf bereits vorhandenen Informationen aufsetzen.

Liberty Alliance

Doch dies erfordert Spezifikationen, Standards und Richtlinien, die den Providern den Austausch dieser Informationen und die Zusammenarbeit unter einem Single Sign-on ermöglichen. Ende Dezember 2001 formierte sich hierfür die „Liberty Alliance“, der Ende 2004

weltweit mehr als 150 Unternehmen, Non-Profit-Organisationen und Regierungsstellen angehören. Sie entwickelt offene Standards für ein föderiertes netzbasiertes Identitätsmanagement (Federated Identity Management).

Basis des Konzepts [38] ist die föderierte Netzidentität (Federated Network Identity) und der Vertrauenszirkel (circle of trust). Die Identität [39] besteht aus Eigenschaften, Attributen und Präferenzen, auf deren Basis der Nutzer personalisierte Services über unterschiedliche Medien erhalten möchte.

Zu den Eigenschaften zählen behördliche Identitäten, wie Ausweis, Pass, Führerschein, Sozialversicherungsnummer, firmenspezifische Identitäten, wie Sign-in-Informationen, und biometrische Merkmale, wie Fingerabdrücke oder Retina-Scans. Zu Attributen und Präferenzen gehören u. a. Reisepräferenzen, wie z. B. Fensterplatz/Gangsitze, Raucher/Nichtraucher, Abteilwagen/Großraumwagen (sogenannte Gegenwörter), aber auch Hobbies, musikalische Präferenzen, z. B. Jazz oder Klassik, Einkaufsvorlieben, Geldanlagepräferenzen, etc. Der Benutzer kann seine föderierte Netzidentität, d. h. sein dortiges persönliches Profil selbst konfigurieren und bestimmen, welchem Provider welche Informationen zugänglich sein sollen.

Service- und Identitäts-Provider [40] bilden auf Basis der Liberty-Technologie einen Vertrauenszirkel und haben Geschäftsvereinbarungen miteinander. Der Vertrauenszirkel ermöglicht den föderierten Austausch spezifischer Nutzerdaten und das Single Sign-on.

Was bedeutet die Umsetzung des Liberty-Konzepts in der Praxis (s. a. [41])? Angenommen, eine Fluggesellschaft, eine Bahnlinie, ein Autovermieter und ein Hotel bilden einen Vertrauenszirkel. Ein Kunde habe bei jedem dieser Unternehmen ein Benutzerkonto mit Benutzerkennung, Passwort und seinem persönlichen Profil. Dieser Kunde möchte nun eine Reise buchen, bei der er per Bahn zum Flughafen fährt, von dort zu seinem Zielort fliegt, für dort einen Wagen mieten und ein Hotel buchen möchte. Er meldet sich bei der Bahnlinie an und ordert ein Ticket. Auf der Webseite der Bahnlinie befinden sich Links zu den Webseiten der anderen Mitglieder des Vertrauenszirkels. Der Benutzer klickt den Link zur Fluglinie an und meldet sich an. Die Fluglinie, weiß, dass er von der Website der Bahnlinie kommt und bietet an, sein Benutzerkonto mit dem der Bahnlinie zu verbinden, so dass er zukünftig nur noch ein einmaliges Sign-on benötigt. Der Kunde kann dies sowohl hier als auch bei den anderen Mitgliedern des Vertrauenszirkels durchführen. Außerdem soll er die Möglichkeit erhalten, festzulegen, wer auf welche Daten zugreifen kann.

Für den Benutzer vereinfacht dies die Pflege seines persönlichen Netzprofils und ermöglicht ihm ein Single Sign-on.

Die Spezifikationsarchitektur [39] für das föderierte Identitätsmanagement der Liberty Alliance besteht aus den folgenden Rahmenwerken:

- Liberty Identity Federation Framework (ID-FF) [40],
- Liberty Identity Web Services Framework (ID-WSF) [42] [43],
- Liberty Identity Services Interface Specifications (ID-SIS) [44].

Sie baut auf bestehenden Standards auf, wie z. B. SAML, http, WSS, WSDL, XML, SSL/TLS, SOAP. Produkte für das föderierte Identitätsmanagement (Federated Identity Management) sind am Markt verfügbar.

9.5.18.7.4 Identitäts- und Access-Management

*Identitäts-
management*

Unabhängig vom föderierten Identitätsmanagement der Liberty Alliance dient das Identitätsmanagement (IdM) in der ITK (Identity Management) allgemein dazu, „digitale“ Identitäten mit ihren zugeordneten realen Personen sowie mit ihren Daten und den dazugehörigen Rechten bezogen auf Ressourcen plattform-, unternehmens- und gegebenenfalls länderübergreifend unter Berücksichtigung des Datenschutzes entlang ihres Lebenszyklus (Identity Life Cycle) zu steuern, d. h. bereit zu stellen, zu verwalten und zu pflegen sowie zu löschen. Der Lebenszyklus unterteilt sich hierbei in die drei Phasen: bereitstellen (provisioning), pflegen (maintaining) und beenden (terminating).

Die Bereitstellung umfasst die Beantragung, Genehmigung und Vergabe, die Pflege beinhaltet Änderungen „persönlicher“ Daten, wie z. B. Änderung, Löschung und Neuvergabe der zugeordneten Rollen und Berechtigungen, aber auch den Namenswechsel nach Heirat und Adressänderungen. Zu verwalten sind neben den Stammdaten oftmals eine Vielzahl zugeordneter Elemente, von den ausgegebenen Schlüsseln, Ausweisen, Chipkarten, Benutzerkonten und Pseudonymen (z. B. E-Mail-Adresse) über Zufahrts-, Zutritts-, Zugangs- und Zugriffsrechten bis hin zu biometrischen Daten.

*Identitäts- und
Access-
management
(IAM)*

Eine effiziente und möglichst sichere zentrale Identitäts-, Rechte- und Regelverwaltung sowie Zugriffssteuerung, wie sie im allgemeinen Sicherheitsschalenmodell nach Dr.-Ing. Müller dargestellt ist, erfordert zusätzlich zum Identitäts- auch ein Accessmanagement. Letzteres ist für die Zugangs- und Zugriffssteuerung zuständig. Ein Identi-

täts- und Accessmanagement (IAM) sollte weitgehend automatisiert und benutzerfreundlich sein.

Dies erfordert u. a. ein geeignetes Rollenmodell sowie einen Workflow für das Antrags-, Genehmigungs-, Vergabe- und Beendigungsverfahren sowie die Anbindung an ein Quellsystem, z. B. ein Personalmanagementsystem, für die Basisdaten und die möglichst automatische rollenbasierte Generierung der Berechtigungen. Außerdem sollte es die Definition von Regeln (policies) ermöglichen, z. B. für die Bildung von Benutzernamen (userid). Ein Single Sign-on empfinden Benutzer dabei als Commodity. Gleichzeitig hilft es, Passwortschreibungen zu vermeiden. Weitere Elemente sind eine Zweifaktorthauthentisierung zur Erhöhung der Sicherheit und ein sicherer Self Service z. B. zum Passwort-Rücksetzen oder zur Veränderung personenbezogener Daten.

Die Vielzahl an Elementen zeigt, dass für den Aufbau des Identitäts- und Accessmanagements umfangreiches Know-how notwendig ist. Ein Unternehmen kann dies entweder selbst aufbauen oder sich durch externe Berater unterstützen lassen. Hinzu kommt, dass Unternehmen ihr IAM üblicherweise nicht auf der grünen Wiese aufbauen können, sondern die bestehende Infrastruktur berücksichtigen und integrieren müssen. Dies erfordert einen Überblick über die vorhandenen Anwendungen sowie je Anwendung und System über die Zuordnung der Benutzer, ihrer Benutzernamen und Rechte sowie die Namenskonventionen. Dies manuell zu erheben und zuzuordnen ist aufwändig und fehleranfällig. Daher sollte hier auf geeignete Werkzeuge zurückgegriffen werden. Doch wenn dies alles so aufwändig ist, welchen Nutzen bietet dann ein solches IAM?

Der zentrale Überblick, die zentrale Verwaltung und Steuerung der Identitäten und Berechtigungen ist ein wesentliches Element der IT-Governance und hilft damit, Compliance-Anforderungen zu erfüllen. Weiterhin stellt es ein entscheidendes Hilfsmittel bei der Prüfung von interner oder externer Seite dar. Außerdem lassen sich kurzfristig und mit überschaubarem Aufwand Reports mit Auswertungen, z. B. über verwaiste Benutzerkonten oder über Zugriffsberechtigungen, ziehen. Ein standardisiertes IAM, unterstützt durch geeignete IAM-Systeme, beschleunigt das Einrichten und Ändern von Identitäten und Berechtigungen. Das automatisierte Einrichten und Ändern von Benutzerkonten entlastet die IT-Administration, reduziert Fehler und kann Missbrauch vermindern. Das Single Sign-on zusammen mit dem Self Service hilft, die Anfragen am Service Desk deutlich zu reduzieren. Da Benutzer ihre Passwörter durch das SSO kaum mehr vergessen, entfallen die Zeiten für das mehrfache Probieren des

IAM: Nutzen

Passwortes, den Anruf beim Service Desk zur Rücksetzung des Passwortes sowie das erneute Einloggen und die Vergabe eines neuen Passwortes.

Dem Nutzen eines IAM steht die Abhängigkeit von dessen Funktionsfähigkeit, Korrektheit und Verfügbarkeit gegenüber. Im Hinblick auf die Handlungsfähigkeit eines Unternehmens stellt das zentrale IAM als Single Point of Failure ein kritisches System dar, dessen Ausfall die Geschäftskontinuität maßgeblich beeinflussen oder ein Unternehmen sogar lahm legen kann.

Software-Lösungen

Software-Lösungen für das zentralisierte Identitäts- und Accessmanagement in Unternehmen sind verfügbar. Bei ihrer Bewertung ist u. a. darauf zu achten, dass sie die Möglichkeit bieten, möglichst viele bestehende Verzeichnisse unterschiedlicher Betriebssysteme, Applikationen und Datenbanken des Unternehmens zu integrieren. Ziel ist es, ein zentrales Benutzer- und Rechteverzeichnis zu erhalten, über das eine plattformübergreifende Administration erfolgt (Single Point of Security Administration), und dem Benutzer gleichzeitig ein Single Sign-on zu ermöglichen.

EU-Forschungsprojekte PRIME und FIDIS

Die zunehmende Bedeutung des Identitätsmanagements unterstreichen zwei Forschungsprojekte, welche die EU im Jahr 2004 aufgesetzt hat. PRIME (Privacy and Identity Management for Europe) – mit einer Laufzeit von 4 Jahren – konzentriert sich auf Lösungen für ein datenschutzförderndes Identitätsmanagement und betrachtet u. a. technische, rechtliche und wirtschaftliche Anforderungen. Ansprechpartner für dieses Projekt ist in Deutschland das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Mit FIDIS (Future of Identity in the Information Society), dem zweiten Forschungsprojekt, soll ein Expertennetzwerk aufgebaut werden. FIDIS, das die Universität Frankfurt am Main koordiniert, hat eine Laufzeit von 5 Jahren.

9.5.18.8 Zufahrtsschutz

Die Zufahrt zum und/oder in das Gebäude sichert der Zufahrtsschutz. Hier ist zu definieren, wer wann mit welchem Fahrzeug und gegebenenfalls welchen Waren wohin Zufahrt erhält und wie dies avisiert und protokolliert wird. Bei Anlieferungen prüft Sicherheitspersonal die Lieferpapiere. Je nach Sicherheitsanforderungen und Sicherheitslage kann dies ergänzt werden um Anlieferungs-, Fahrzeug- und Personenkontrollen.

9.5.18.9 Zutrittsschutz

Zum Gebäude und den Räumlichkeiten eines Unternehmens existiert üblicherweise ein Zutrittsschutz und sei es auch nur in Form einer abschließbaren Eingangstür. Je mehr Mitarbeiter zu einem Unternehmen gehören, desto weniger praktikabel ist diese Lösung. Unternehmen setzen daher Zutrittsverfahren und elektronische Zutrittskontrollsysteme (ZKS) ein, um nur autorisierten Personen Zutritt zu sicherheitsrelevanten Räumlichkeiten zu gewähren.

Die Stärke des Zutrittsschutzes und der Begrenzung der Zutrittsberechtigten sind weitere Aspekte. Sie korrespondieren in der Regel mit dem Schutzbedarf der Räumlichkeiten. Entsprechend den Sicherheitsanforderungen erfolgt eine Zuordnung der Räumlichkeiten in unterschiedliche Sicherheitsklassen.

Sicherheitsklassen

In einem Gebäude befinden sich häufig Räumlichkeiten, die zu unterschiedlichen Sicherheitsklassen gehören. Dementsprechend ergeben sich im Gebäude Bereiche mit unterschiedlichen Sicherheitsanforderungen, sogenannte Sicherheitszonen. Je sicherheitskritischer Räumlichkeiten sind, desto stärker sollten sie abgesichert und in das sicherere Gebäudeinnere verlagert werden.

Sicherheitszonen

Als Standard-Zutrittsschutz setzen Unternehmen oftmals ein Zutrittskontrollsystem mit Türen, Drehkreuzen oder Drehsperrern und Magnet- bzw. Chipkartenleser ein. Die Zutrittsberechtigung für die Mitarbeiter beschränken die Unternehmen dabei, dem Prinzip der minimalen Rechte folgend, auf einzelne Standorte, Gebäude, Gebäudeabschnitte oder Etagen sowie auf bestimmte Zeiten, z. B. nur werktags von 7:00 Uhr bis 20:00 Uhr.

Standard-Zutrittsschutz

Den Zutritt zu Räumlichkeiten mit einem sehr hohen Schutzbedarf regeln oftmals Vereinzelungsanlagen, so dass nur eine einzelne Person mit entsprechenden Zutrittsrechten in den jeweiligen Raum gelangen kann.

Starker Zutrittsschutz

Für sicherheitsrelevante Räumlichkeiten existieren je nach Schutzbedarf zusätzliche Zutrittskontrollsysteme. Was sind nun sicherheitsrelevante Räumlichkeiten? Dies sind Räume, die einen höheren Schutzbedarf haben und zu denen nur ein eingeschränkter Kreis von Mitarbeitern standardmäßig Zutritt erhält. Solche sicherheitsrelevanten Räumlichkeiten sind

- aus Geschäftsprozesssicht z. B.
 - bei Banken die Handelsräume
 - in der Industrie die Forschungs- und Entwicklungsabteilungen

- aus Sicht der Datenverarbeitung die Rechenzentren und Serverräume
- aus Telekommunikationssicht z. B. die Räume mit der Telekommunikationsanlage und aktiven bzw. passiven kommunikationstechnischen Komponenten, wie Hubs, Router, Gateways etc.
- aus versorgungstechnischer Sicht z. B. die Räume mit der Netzersatzanlage, der Trafostation und der unterbrechungsfreien Stromversorgung.

Zusätzliche Zutrittsschutzmaßnahmen für sicherheitsrelevante Räumlichkeiten sind im einfachsten Fall abgeschlossene Räume, deren Schlüssel nur wenige autorisierte Personen besitzen bzw. zu denen nur wenige autorisierte Personen Zutritt haben. Andere Maßnahmen des Zutrittsschutzes sind bei Rechenzentren beispielsweise Vereinzelungsanlagen, die über ein Zutrittskontrollsystem verfügen, bei dem die Zutrittsberechtigungsprüfung z. B. auf einem der folgenden Wege erfolgt:

- über Fingerabdruck und PIN
- über Magnetkarte/Chipkarte und PIN
- über Magnetkarte/Chipkarte und biometrisches Merkmal, z. B. Fingerabdruck, Gesicht, Iris.

Neben den Zutrittskontrollsystemen müssen Verfahren für die Ausstellung von Ersatzausweisen und Besucherausweisen sowie Zutrittsregelungen für Dienstleister, Handwerker, Wartungs- und Reinigungspersonal definiert sein. Hierbei ist zu beachten, dass Personen, die temporären Zutritt zu sicherheitsrelevanten Räumlichkeiten erhalten sollen, z. B. entsprechend überprüft, begleitet und über Sicherheitsbestimmungen informiert werden.



Umgangener Zutrittsschutz durch unzureichendes Sicherheitsbewusstsein

Im Rahmen einer Sicherheitsuntersuchung durfte ich mich im Gebäude eines Unternehmens frei bewegen. Ziel war es, den Zutrittsschutz zu sicherheitsrelevanten Räumlichkeiten zu umgehen. In einem zutrittsgeschützten Großraum wurde einer der Kerngeschäftsprozesse des Unternehmens abgewickelt. Um in diesen Raum zu gelangen, schloss ich mich einem mir unbekannten Mitarbeiter des Unternehmens an, der sich auf diesen Raum zubewegte. Ich stellte mich hinter ihm an, als er die Tür mittels seiner Berechtigung öffnete. Er hielt mir die Tür auf und ich betrat den Raum. Während ich den Raum durchschritt, sah ich eine Tür, die anscheinend in einen Nachbarraum führte. Die Tür war nicht verschlossen. Ich öffnete sie und stand in einem Serverraum, über den alle dortigen Arbeitsplätze mit ITK versorgt wurden.

Grenzenlose Freiheit

Kennen Sie das oder Ähnliches auch? Der Zutritt zu einem Rechenzentrum ist über eine Vereinzelungsanlage, Kameraüberwachung und Wachpersonal geschützt. Sie kommen nur nach einer Sicherheitsüberprüfung hinein – bis 18:00 Uhr. Dann wird ein Nebeneingang für längere Zeit geöffnet, über den das Reinigungspersonal in das und aus dem Rechenzentrum gelangen und sich dort frei bewegen kann.

9.5.18.10 Zugangsschutz

Um den Zugangsschutz zu Anwendungen und Netzen abzusichern, führen Sicherheitsbeauftragte eine Pfadanalyse durch, in der sie die verschiedenen Zugangspfade ermitteln, klassifizieren und entsprechend absichern.

Pfadanalyse

Zum Zugangsschutz etablieren sie Sicherheitsmaßnahmen zur bereits übergreifend geschilderten Identifikation und Authentisierung.

Zugangsschutz

Den Zugang über „nicht vertrauenswürdige“ Netze lassen Sicherheitsbeauftragte durch eine zusätzliche Barriere in Form von Firewalls schützen. Wer eine weiter gehende kontinuierliche Überwachung des Datenverkehrs und die Erzeugung von Meldungen möchte, plant Intrusion-Detection- und -Response-Systeme ein.

*Firewall,
Intrusion-
Detection- und
- Response-
Systeme*

Als weiteres Sicherheitselement lassen Sicherheitsbeauftragte z. B. Content-Security-Systeme implementieren, um den Inhalt von Nachrichten prüfen lassen zu können.

*Inhaltsprüfung
durch Content-
Security-
Systeme*

Viren-Suchprogramme schließlich nutzen sie zur Erkennung und Abwehr von Computerviren.

Virenschutz

Detailliertere Ausführungen zu Firewalls, Intrusion-Detection- und -Response-Systemen, Content-Security-Systemen und Computerviren-Suchprogrammen finden Sie im Kapitel Sicherheitsarchitektur unter Ressourcen.

9.5.18.11 Zugriffsschutz

Der Zugriff auf die Ressourcen der ITK muss geschützt werden, damit nur autorisierte Personen Daten, z. B. Personaldaten, einsehen können und nur berechtigte Personen Veränderungen bzw. Neueingaben vornehmen können.

Für den Aufbau eines Zugriffsschutzes sind verschiedene Informationen notwendig, die sich aus folgender Frage ergeben:



Wer soll worauf welchen Zugriff erhalten?

Zugriff erhalten sollen Subjekte, z. B. Personen oder Anwendungen. Das, was geschützt werden soll, sind die Objekte, oder auch Ressourcen. Die Art des Zugriffs ist durch Rechte, z. B. lesen, ändern, einfügen, löschen, ausführen, gekennzeichnet. Es ergibt sich somit das Subjekt-Recht-Objekt-Modell.

Hieraus folgt, dass für jedes Subjekt definiert werden muss, mit welchen Rechten es auf welches Objekt zugreifen darf. Es ergibt sich der bereits erwähnte „Berechtigungswürfel“ oder „Berechtigungskubus“.



Deutschland: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Gemäß GDPdU muss der Steuerpflichtige dem Prüfer der Finanzbehörde drei Arten des Datenzugriffs gewähren:

- Unmittelbaren Datenzugriff
- Mittelbaren Datenzugriff und
- Datenträgerüberlassung

Beim unmittelbaren Datenzugriff muss der Steuerpflichtige durch geeignete Zugriffsbeschränkungen sicherstellen, „dass der Prüfer nur auf steuerlich relevante Daten des Steuerpflichtigen zugreifen kann“.

Um die Komplexität zu reduzieren und die Verwaltung zu vereinfachen, bilden die Ressourcenverantwortlichen in Abstimmung mit dem Sicherheitsbeauftragten und der Revision Gruppen. Diese Gruppenbildungen können sich sowohl auf der Subjekt- als auch auf der Objektseite vollziehen. Es entstehen Subjektgruppen, z. B. Benutzergruppen, und Objektgruppen, Ressourcengruppen. Darüber hinaus kann die dreidimensionale Darstellungsweise in eine zweidimensionale, die so genannte Berechtigungsmatrix, reduziert werden, wenn die Rechte nicht in z-Richtung aufgetragen, sondern in Form von Einträgen in die Matrixfelder dargestellt werden.

9.5.18.12 Leseschutz

*Verschlüsselung,
Kryptographie,
Chiffrierung*

Um Nachrichten und Daten vor unberechtigter Kenntnisnahme und Manipulation zu schützen, lässt sich die Verschlüsselung (Chiffrierung, Kryptographie) einsetzen. Hierbei transformiert ein festgelegtes Verfahren (Algorithmus) unter Einsatz eines „Schlüssels“ oder Codes die zu verschlüsselnden Informationen in einen Geheimtext (Chiffre). Für die Sicherheit der Verschlüsselung ist es wesentlich, dass das Verfahren und eventuelle unterstützende Hilfsmittel, wie z. B. Software-Tools, offen gelegt werden und überprüfbar sind. Der Schlüssel

selbst muss geheim gehalten werden. Die Rückgewinnung der Information aus dem Geheimtext heißt Entschlüsselung (Dechiffrierung). Ohne den Schlüssel darf es Unbefugten nicht möglich sein, den Geheimtext zu entschlüsseln.

Mit der Kryptographie werden folgende Ziele verfolgt:

*Ziele der
Kryptographie*

1. Vertraulichkeit/Geheimhaltung: Der Inhalt einer Nachricht oder Datei soll vor Unberechtigten verborgen bleiben.
2. Integrität/Unverändertheit: Die unbefugte Manipulation einer Nachricht oder Datei soll entdeckt werden können.
3. Authentizität/Echtheit: Ein Kommunikationspartner soll Folgendes beweisen können:
 - a) seine Identität
 - b) seine Urheberschaft und die Unverändertheit seiner Nachricht.
4. Verbindlichkeit/Nichtabstreitbarkeit: Ein Kommunikationspartner soll Folgendes nicht abstreiten können:
 - a) den Versand einer Nachricht
 - b) den Empfang einer Nachricht.

Diese Ziele lassen sich mit geeigneten Verschlüsselungsverfahren erreichen. Es werden folgende Verschlüsselungsverfahren unterschieden:

1. symmetrische
2. asymmetrische

Symmetrische Verschlüsselungsverfahren verwenden ein und denselben Schlüssel zur Ver- und Entschlüsselung. Sie werden daher auch als „Ein-Schlüssel“-Verfahren bezeichnet. Vor der Nutzung eines symmetrischen Verschlüsselungsverfahrens müssen die Kommunikationspartner den Schlüssel auf einem „sicheren“ Kanal ausgetauscht haben. Bekannte symmetrische Verschlüsselungsverfahren sind DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard) [45], IDEA™ (International Data Encryption Algorithm) und RC5™ [46]. Sie gehören zur Gruppe der Blockchiffren, weil jeder Verschlüsselungstakt einen ganzen Block von Bits verschlüsselt.

*Symmetrische
Verschlüs-
selungs-
verfahren*

Symmetrische Verschlüsselungsverfahren sind relativ schnell und daher zur Onlineanwendung geeignet. Sie bieten bei verhältnismäßig kurzer Schlüssellänge eine hohe Sicherheit. Die Stärke der Verschlüsselung wird im Wesentlichen durch die Schlüssellänge bestimmt. Da jedoch jeder der Kommunikationsteilnehmer für jeden Kommunikationspartner einen eigenen Schlüssel benötigt, wird die Verwaltung dieser Schlüssel schnell umständlich.

Eigenschaften

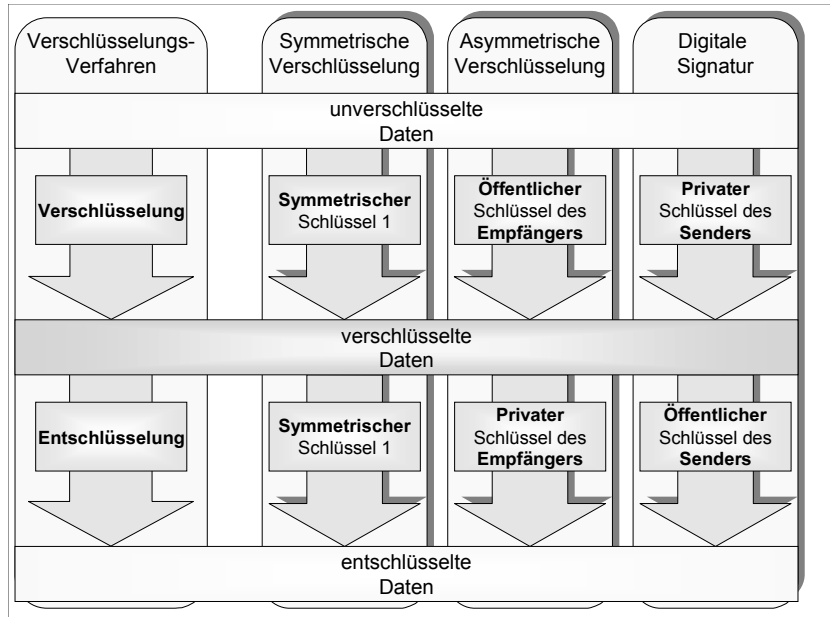


Abb. 9.14: Verschlüsselungsverfahren

*Asymmetrische
Verschlüs-
selungs-
verfahren*

Asymmetrische Verschlüsselungsverfahren (Public-Key-Verfahren) benutzen zwei verschiedene, aber zusammengehörende Schlüssel. Der „öffentliche“ Schlüssel (Public Key) dient der Verschlüsselung, der „private“ der Entschlüsselung. Während der „öffentliche“ Schlüssel bekannt gemacht wird, muss der „private“ Schlüssel geheim gehalten werden. Eine Entschlüsselung darf nur mit dem „privaten“ Schlüssel möglich sein. Außerdem ist sicherzustellen, dass der „öffentliche“ Schlüssel nachweisbar zum Empfänger gehört, da ansonsten Schlüssel von Unbefugten untergeschoben werden könnten. Deshalb ist eine vertrauenswürdige dritte Partei (Zertifizierungsstelle, Trust Center) erforderlich, welche die Echtheit des öffentlichen Schlüssels des Empfängers mit einem „Zertifikat“ bestätigt. Letzteres wird meist ebenfalls durch ein kryptographisches Verfahren erzeugt und dem öffentlichen Schlüssel beigelegt. Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist das nach Rivest, Shamir und Adleman benannte RSA-Verfahren.

Eigenschaften

Bei asymmetrischen Verfahren muss jeder Teilnehmer nur einen Schlüssel geheim halten. Sie eignen sich gut für die digitale Signatur (elektronische Unterschrift) und für Verbindlichkeitsnachweise. Nachteilhaft ist, dass sie langsam und leichter attackierbar sind. Sie be-

nötigen daher im Vergleich zu symmetrischen Verfahren relativ lange Schlüssel. Zusätzlich ist die Schlüsselerzeugung in der Regel aufwändig.

Hybride Verfahren sollen die Vorteile der symmetrischen und asymmetrischen Verschlüsselung in sich vereinen. Hierzu übermitteln die Kommunikationspartner z. B. den Sitzungsschlüssel für eine symmetrische Verschlüsselung in asymmetrisch verschlüsselter Form. Die Massendaten verschlüsseln sie anschließend mit dem schnelleren symmetrischen Verfahren.

*Hybride
Verfahren*

Die folgende Tabelle ordnet den jeweiligen Verfahren in der Praxis vorkommende Standards zu:

Verfahren	Standard
Symmetrisch	DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard), IDEA™ (International Data Encryption Algorithm) RC5™
Asymmetrisch	RSA (Rivest Shamir Adleman)

In der Praxis sind Verschlüsselungsprogramme (Krypto-Tools) anzutreffen, die Nachrichten und Dateien ver- und entschlüsseln sowie mit einer digitalen Signatur versehen können. Derartige Programme implementieren üblicherweise Funktionen des OpenPGP-Standards [47].

*Verschlüs-
selungs-
programme*

Datenträgerverschlüsselung



Mit zunehmender Mobilität der Nutzer steigt die Gefahr, dass die von ihnen genutzten mobilen Endgeräte, wie z. B. Notebooks, PDAs oder USB-Memory-Sticks sowie handtellergröße portable USB-Mini-Festplatten mit einigen zehn Gigabyte, gestohlen werden oder verloren gehen. Dies stellt eine Bedrohung für die Vertraulichkeit der darauf befindlichen Daten dar. Dementsprechend empfiehlt es sich, sensitive Daten verschlüsselt zu speichern. Hierbei ist die Verfügbarkeit des Schlüssels ebenso sicherzustellen wie die Praktikabilität des Handlings im Hinblick auf die Bedienung und die Zeitdauer der Ver- und Entschlüsselung.

USB-Memory-Sticks erfreuen sich nach meinen Erfahrungen zunehmender Beliebtheit. Für vertrauliche Daten gibt es einen USB-Memory-Stick, bei dem die Authentisierung des Benutzers über einen eingebauten Fingerabdruck-Sensor erfolgt. Bei Geräten, die eine Authentisierung mittels Fingerabdruck oder anderer biometrischer Merkmale unterstützen sind die False Acceptance Rate (FAR) und die False Rejection Rate (FRR) in die Sicherheitsbewertung mit einzubeziehen.

Steganografie Steganografie stellt eine Möglichkeit dar, Nachrichten unbemerkt und vertraulich zu übermitteln. Hierzu wird die vertrauliche Nachricht versteckt, z. B. in einer anderen Nachricht. Bekannte Methoden für derartige unbemerkt übermittelte Informationen sind die Mikropunkte, die im Zweiten Weltkrieg genutzt wurden, oder die unsichtbare Tinte. Heutzutage lassen sich geheime Informationen in harmlos erscheinenden Nachrichten, z. B. Bildern in Form einer GIF-Datei, verbergen.

9.5.18.13 Wiederaufbereitung

Die Wiederaufbereitung soll dafür sorgen, dass Informationsträger, wie z. B. Speichermedien, vor ihrer anderweitigen Nutzung so gelöscht sind, dass keine Rückschlüsse auf ihren ursprünglichen Inhalt möglich sind. Hierbei ist zu beachten, dass Dateisysteme beim Löschvorgang üblicherweise nur den Verzeichniseintrag löschen, während die physikalischen Daten weiter erhalten bleiben. Daher müssen Fest- und Wechsellplatten, USB Memory Sticks, Disketten, CD-ROMs, DVDs und Datenbänder vor ihrer Entsorgung physikalisch vollständig gelöscht oder sogar zerstört sein, um unautorisierte Zugriffe auf die Daten zu verhindern.

Ein physikalischer Löschvorgang kann durch (mehrfaches) Überschreiben der Daten erfolgen oder durch Daten- bzw. Datenträgervernichtung.

*Überschreibende
Löschtools*

Bei den überschreibenden Löschtools gibt es solche, die einzelne Dateien des Dateisystems überschreiben können, gegebenenfalls einschließlich freier Speicherbereiche, und solche, die die Festplatte oder Partition nur komplett löschen können. Je nach Tool werden die Löschvorgänge in einem Protokoll dokumentiert.

Für das Löschen selbst gibt es unterschiedliche Verfahren, die sich primär in der Art des/der Muster und der Anzahl der Schreibvorgänge unterscheiden. Hierzu gehören Verfahren von Peter Gutmann, von Bruce Schneier und vom Bundesamt für Sicherheit in der Informationsverarbeitung sowie die Standards DoD 5220.22-M, das NSA DoD 5220.22-M ECE und das NAVSO P-5239-26. Das Löschverfahren von Gutmann [48] mit 35 Überschreibvorgängen und achtmaliger Verwendung von Zufallszahlen dürfte sehr hohen Sicherheitsansprüchen genügen, auch im Hinblick auf Methoden der forensischen Analyse.

*Daten-
vernichtung*

Zu den physikalischen Datenvernichtern gehören für magnetische Datenträger die „De-Gausser“, welche die Platte oder das Band einem magnetischen Wechselfeld aussetzen.

Bei der Datenträgervernichtung lassen sich mechanische, thermische und chemische Verfahren unterscheiden. Zu den mechanischen Verfahren gehört das Schreddern. So können optische Datenträger in Schreddern gemäß DIN 32757 zur Vernichtung von Informationsträgern zermahlen werden. Thermische Verfahren sind das Einschmelzen oder Verbrennen des gesamten Datenträgers. Ein chemisches Verfahren besteht im Wegätzen der Speicherfläche.

*Mechanische,
thermische und
chemische
Datenträger-
vernichtung*

9.5.18.14 Absendekontrolle

Die Absendekontrolle soll – soweit möglich – vermeiden, dass geheime, vertrauliche oder interne Informationen das Unternehmen unbeabsichtigt oder unverschlüsselt verlassen. Darüber hinaus soll sie verhindern, dass das Unternehmen Schadsoftware versendet und von ihm Attacken oder Spam-Mails ausgehen. Dies erfordert beispielsweise ein Scannen ausgehender E-Mails auf Viren und Schlagwörter, z. B. „vertraulich“ oder „geheim“, und die Verhinderung von „E-Mail-Fluten“ zu einer Zieladresse. Im Hinblick auf Spamming ist die Konfiguration des SMTP-Ports hinreichend sicher zu gestalten und zu testen, so dass Angreifer die unternehmenseigenen Server nicht als Zwischenstation (Relay) für Spam-Mails missbrauchen können [49].

9.5.18.15 Übertragungssicherung

Daten oder Informationen lassen sich über eine Vielzahl von Medien vom Papier über drahtgebundenen bis hin zu drahtlosem Daten- und Informationsaustausch übertragen. Die Übertragung kann im einfachsten Fall bei Gesprächen vis-à-vis oder über Telefon bzw. Handy erfolgen, aber auch über Fax, E-Mail, SMS, MMS, Datenträgeraustausch, elektronischen Datenaustausch, z. B. mittels EDI, EDIFACT, ebXML etc. Während der Übertragung müssen die Daten der jeweiligen Sicherheitsstufe entsprechend geschützt werden. Zum Schutz der Übertragung dient die Übertragungssicherung.

Drahtlose Übertragungen bergen u. a. die potenzielle Gefahr des Abhörens in sich. Hierzu gehören nicht nur WLANs, sondern z. B. auch drahtlose Übertragungen von Telefonen, Tastaturen und Überwachungskameras. Aber auch drahtgebundene Übertragungen können Angreifer abhören, beispielsweise durch Sniffer, welche die Leitung abhören, oder Key-Logger, welche die Tastatureingaben miterschneiden. Die verschlüsselte Übertragung von Daten spielt sowohl in der unternehmensinternen und –externen Datenübertragung zwischen Computern eine Rolle, als auch bei der Übertragung von Daten zu Druckern und von Scannern.

Im Bereich der Übertragungssicherung spielen die Sicherheitskriterien Vertraulichkeit, Integrität und Verbindlichkeit im Hinblick auf Angriffe eine wesentliche Rolle. Um diese Sicherheitskriterien zu schützen, sind beispielsweise folgende Verfahren möglich:

Kriterium	Verfahren
Vertraulichkeit	Verschlüsselung (Kryptographie)
Integrität	Checksum, Digitale Signatur
Verbindlichkeit	Digitale Signatur

9.5.18.16 Abgangskontrolle

Die Abgangskontrolle soll erreichen, dass nur diejenigen Objekte das Unternehmen verlassen, die dies auch dürfen. Dies betrifft physisches Eigentum des Unternehmens, d. h. die Schutzobjekte, z. B. PCs, Speicherkarten, Disketten, CD-ROMs, DVDs, USB-Memory-Sticks, portable USB-Mini-Festplatten, Festplatten sowie papierhafte Unterlagen. Aufgrund der Mobilität, der Miniaturisierung und Tarnung wachsen hier die Anforderungen, wie Schweizer Messer mit integriertem USB-Memory-Stick und handtellergroße portable USB-Festplatten zeigen. Die Intensität der Abgangskontrolle ist abhängig von den Sicherheitsanforderungen und der aktuellen Sicherheitsstufe.

9.5.18.17 Transportsicherung

Unter Transportsicherung sind Konzepte und daraus abgeleitete Maßnahmen zu verstehen, die den Transport von Werten, z. B. Datenträgern und Dokumenten, schützen sollen. Zu diesen Sicherheitsmaßnahmen gehören beispielsweise die Auswahl des Transportunternehmens und die Wahl einer geeigneten, d. h. angemessen gesicherten Transportart, verschlüsselte Daten, gesicherte Behältnisse und Fahrzeuge, sicherheitsüberprüftes Begleitpersonal und eine entsprechende Organisation.

9.5.18.18 Abfahrtskontrolle

Die Abfahrtskontrolle soll sicherstellen, dass nur solche Objekte oder Werte aus dem Unternehmen herausgefahren werden, für die dies erlaubt ist. Das unzulässige Abtransportieren beispielsweise von Eigentum oder gefährlichen Substanzen soll dadurch vermieden werden.

9.5.18.19 Alarmierung

Für die Überwachung der Sicherheitsschalen ist es erforderlich, dass bei Sicherheitsverletzungen ein Alarm ausgelöst wird. Sowohl die Alarmer als auch die Protokolle sollten Angaben darüber enthalten, wer wann wo welche Aktivität ausgeführt hat. Hierdurch gibt es beispielsweise Informationen darüber, wer wann von wo auf welche Daten welchen Systems mit welchem Erfolg zugegriffen hat, Zugang zu welchem Netz erlangt hat oder den Zutritt zu welchem Raum gesucht hat.

9.5.18.20 Protokollierung und Beweissicherung

Protokollierung (logging) ist ein in vielerlei Hinsicht heikles Thema: Die Benutzer befürchten Beobachtung, der Betriebsrat/Personalrat vermutet Leistungsmessung, die Systembetreuer erschrecken vor riesigen Datenmengen und Stapeln auszuwertender Protokolle.

Diese Aspekte gilt es bei der Protokollierung zu berücksichtigen. Es müssen daher Repräsentanten aller betroffenen Gruppen in die Konzeptentwicklung mit einbezogen werden. Durch deren Beteiligung lässt sich Akzeptanz schaffen und eine angemessene Lösung finden. Diese wird als Sicherheitsrichtlinie festgehalten.

Akzeptanz

Bei der Definition der Schutzbedarfsklassen sollte bereits festgelegt worden sein, welche Daten standardmäßig zu protokollieren sind. Der jeweilige Einzelfall erfordert dann nur noch eine Überprüfung. Andernfalls wird unter Berücksichtigung der Sicherheitsklasse des Schutzobjekts in einem ersten Schritt festgelegt, dokumentiert und kommuniziert, warum protokolliert werden soll. Im nächsten Schritt werden die Ereignisse festgelegt, die zu welchem Zweck und mit welchen Daten protokolliert werden sollen. Ebenfalls festgelegt wird, welche weiter gehenden Maßnahmen, z. B. Alarmierung, ausgelöst werden sollen.

Vorgehen

Sicherheitsrelevante Ereignisse können z. B. sein:

- Zufahrt/Zufahrtsversuche zu Bereichen
- Zutritte/Zutrittsversuche zu Räumlichkeiten
- Zugänge/Zugangsversuche zu Rechnern und Netzen
- Zugriffe/Zugriffsversuche auf Daten.

*Sicherheits-
relevante
Ereignisse*

Diese sicherheitsrelevanten Ereignisse werden häufig weiter detailliert. Beispielsweise wird festgelegt, ab welcher Sicherheitsklasse welche Zugriffe auf Daten protokolliert werden.

Darüber hinaus werden privilegierte Operationen, wie z. B. Supervisor-Aktivitäten, Start und Stopp des Computersystems, Anbindung

oder Freigabe von Ein-/Ausgabeeinheiten, sowie versuchte Zufahrts-, Zutritts-, Zugangs- und Zugriffsverletzungen protokolliert.

9.5.18.21 Protokollauswertung und Berichtswesen

*Protokoll-
auswertung*

Die protokollierten Daten in den Log-Dateien müssen in regelmäßigen Zeitabständen ausgewertet werden. Hierzu ist festzulegen, wer diese Daten einsehen darf sowie wer wann und in welchem Zyklus Auswertungen unter Nutzung welcher Hilfsmittel durchführen darf.

Berichtswesen

Über die Ergebnisse der Auswertungen sollten regelmäßig Berichte erstellt werden. Diese sollten Statistiken und Trendkurven beinhalten, um u. a. Status, Kosten und Nutzen verfolgen zu können.

*Forensische
Informatik*

Zusätzlich zu den regulären Protokollauswertungen können ereignisgesteuerte Auswertungen von Log-Dateien erforderlich sein. Hat beispielsweise ein Angriff stattgefunden, so stellen sich die Fragen: Wie konnte der Angreifer in das System gelangen? Was hat der Eindringling in welcher Reihenfolge gemacht? Seit wann ist er auf dem System? Welche Tools nutzte er? Von wo kam der Angriff? Um Antworten auf diese Fragen zu finden, gibt es die forensische Informatik, auch als forensische Computeranalyse oder Computerforensik bezeichnet.

*Forensisch =
gerichtlich*

Was bedeutet das Wort „forensisch“? Es ist gleichbedeutend mit gerichtlich. Dieser fachsprachliche Begriff wird insbesondere im Zusammenhang mit der Gerichtsmedizin (forensische Medizin bzw. Forensik) verwendet. Die forensische Chemie als Teilgebiet der Rechtsmedizin widmet sich der Aufklärung von Verbrechen durch chemische Spurenanalyse. Dementsprechend beschäftigt sich die forensische Informatik mit der Spurensuche auf Computern bzw. IT-Komponenten nach erfolgreichen Angriffen.

Forensische Untersuchungen an Computern bestehen aus:

1. der Datenzusammenstellung und
2. der Analyse.

Im ersten Schritt stellt der forensische Sachverständige bitgenaue Kopien der relevanten Datenträger her und schützt sie vor Veränderungen. Dies kostet jedoch Zeit. Um die Untersuchung früher beginnen zu können, gibt es eine spezielle Hardware-Komponente, die zwischen die Festplatte und deren Controller geschaltet wird. Sie verhindert Schreibzugriffe auf das Untersuchungsobjekt und leitet sie stattdessen auf die eigene Festplatte um. Dadurch lässt sich der Kopiervorgang vermeiden. Wie auch beim bitgenauen Kopieren der Festplatte muss das System jedoch heruntergefahren werden. Dann

erfolgt der Einbau der speziellen Hardware-Komponente und das Hochfahren des Systems.

Im zweiten Schritt untersucht der forensische Experte im Rahmen einer Post-Mortem-Analyse die Kopien bzw. am laufenden System das schreibgeschützte Original. Hierbei nutzt er Tools, deren Namen teilweise ebenfalls an die Gerichtsmedizin erinnern, wie z. B. „The Coroner’s Toolkit“ [50]. Aus Gründen der Gerichtsfestigkeit muss der Sachverständige sicherstellen, dass er das Untersuchungsobjekt, die Festplatte, im Rahmen der Analyse nicht verändert.

Die Analyse erstreckt sich insbesondere auf die Schwachstelle, die der Angreifer nutzte, die Aktivitäten, die er ausgeführt hat, den zeitlichen Ablauf des Angriffs und die eingesetzten Tools. Ebenfalls wichtig ist es, herauszufinden, ob sich der Eindringling (Intruder) Hintertüren geschaffen hat, über die er sich zu einem späteren Zeitpunkt leicht Zugang zum System verschaffen kann. Im Rahmen der Analyse versucht der forensische Informatiker, gelöschte Dateien zu ermitteln und – soweit möglich – zu rekonstruieren. Erschwert wird ihm die Analyse dadurch, dass Angreifer in der Regel versuchen, Ihre Spuren zu verwischen, indem sie z. B. Protokolldateien verändern, oder keine Spuren zu hinterlassen.

Eine Vorgehensweise des Angreifers besteht dementsprechend darin, Spuren auf der Festplatte möglichst zu vermeiden. Dies ermöglichen (Remote) Code-Injection-Attacken. In diesem Fall nutzt der Angreifer eine ihm bekannte Schwachstelle, z. B. Buffer-Overflow, zur Korruption des Speichers (memory) aus. Hierbei bringt er eingeschleusten Code im flüchtigen Prozessspeicherbereich zur Ausführung, um im ersten Schritt vorhandene Schutzsubjekte, wie beispielsweise Firewalls, zu umgehen. Der Code ermöglicht es dem Angreifer, anschließend weitere Kontrolle über das System zu erlangen. Durch Remote Code Injection lassen sich auch DLLs (Dynamic Link Library), die sich im Prozessspeicher befinden, verändern (DLL Injection), ohne dass dies zu deren Änderung auf der Festplatte führt. Wegen der fehlenden Spuren auf der Festplatte hilft das zuvor geschilderte Verfahren eines Abbildes der Festplatte zur späteren Analyse nicht weiter. Was ist zu tun?

Als Antwort hierauf haben forensische Informatiker die Live-Analyse entwickelt. Sie bezieht die Sammlung und Analyse flüchtiger Daten in die forensische Untersuchung mit ein. Hierzu sichern die Informatiker die Inhalte flüchtiger Speicher über entsprechende Speicher-dumps (Speicherkopien) für die anschließende Analyse. Würde der Dump auf die vom System genutzte Festplatte geschrieben werden,

wären deren Inhalte verfälscht. Daher erfolgt dessen Speicherung beispielsweise auf dem im Netz befindlichen Analyserechner.



Forensische Codes

Forensische Codes hat die Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) in Ausdrucken von Laserfarbdruckern entdeckt. In Gittern aus 15 x 8 winzigen gelben Punkten sind Datum und Uhrzeit sowie die Seriennummer des Druckers codiert. Dieser Code soll als Sicherheitsmaßnahme gegen Geldfälscher dienen und die Suche unterstützen.

9.5.19 Architekturmanagement (Architecture Management)

Die Architektur und hierbei insbesondere die Sicherheitsarchitektur eines Unternehmens muss mit den Umfeldveränderungen Schritt halten. Sie entwickelt sich daher aufgrund neuer Erkenntnisse, externer Anforderungen und technologischer Veränderungen kontinuierlich weiter. Der hierzu erforderliche Prozess heißt Architekturmanagement. Welche Aufgaben hat dieser Prozess?

Er sorgt für die Dokumentation der aktuell festgelegten Architekturelemente sowie der aktuellen Architektur. Das Architekturmanagement plant zukünftige Architekturelemente und Architekturen und entwickelt Strategien für die Überführung der aktuellen in die zukünftige Architektur. Dies schließt die zeitliche Betrachtung sowie die Planung aller erforderlichen Ressourcen bis hin zu finanziellen Mitteln ein. Die Architektur umfasst alle PROSim-Elemente. Hierzu gehören u. a. die Prozess-, System-, Anwendungs- und Skillarchitektur sowie die Netztopologie. Außerdem fließen hier die Sicherheitsarchitektur sowie die Schadens-, Bedrohungs- und Risikoarchitektur des Risikomanagements ein.

9.5.19.1 Serviceorientierte Architektur

Service-orientierte Architektur (SOA)

Ein aktuelles Thema im Architekturmanagement ist die serviceorientierte Architektur (Service Oriented Architecture {SOA}) [25]. Sie hat das Potenzial, sich zum künftigen Programmierkonzept für Anwendungen zu entwickeln. SOA besteht aus modularen voneinander unabhängigen und lose miteinander gekoppelten Services, deren Eigentümer unterschiedlich sein können. Ihre Ausgestaltung orientiert sich an den Anforderungen der Geschäftsprozesse, also nicht an der IT, sondern an der Geschäftslogik.

Orchestrierung

Eine gewünschte Geschäftslogik bzw. Funktionalität realisiert SOA durch die Orchestrierung, d. h. die Zusammenstellung von Services und ihre Abfolge. Dies reduziert die Neuentwicklung. So sollen erfolgskritische Kernprozesse, die zum Erhalt des Innovationsvor-

sprungs kontinuierlich anpassbar und schnell änderbar sein sollen, zeitnäher in Produktion gehen können. Die Kunst besteht hierbei darin, die Dienste so festzulegen, dass sie sich als Bausteine zur Realisierung unterschiedlicher Geschäftslogiken bzw. Funktionalitäten nutzen lassen. Damit stellt sich eine vergleichbare Aufgabe wie in der Objektorientierung, bei der es um die Konzeption geeigneter Objekte geht.

Die Services lassen sich über standardisierte Schnittstellen, die Service Interfaces, miteinander verknüpfen. Die Kommunikation der Services untereinander heißt Konversation. Hierbei merkt sich der jeweilige Service den Status, in dem er sich innerhalb einer Interaktion beim Austausch mehrere Nachrichten befindet.

Konversation

Die Choreografie schließlich beschreibt die Abfolge der Nachrichten. Das World Wide Web Konsortium (W3C®) erläutert in seinem Web Services Glossary vom 11. Februar 2004, dass Transaktionen zwischen Web Services aus verschiedenen einzelnen Interaktionen zusammengesetzt sein können. Diese Komposition aus Interaktionen, ihre Nachrichtenprotokolle und Schnittstellen, ihre Reihenfolge und die damit verbundene Logik definiert das W3C® als Choreographie

Choreographie

Der Einsatz weitgehend vorhandener, erprobter, standardisierter und (hoffentlich) sicherer Services unterstützt die Agilität eines Unternehmens und erhöht dessen Flexibilität. Gleichzeitig verringern erprobte Services die Entwicklungszeiten und das potenzielle Fehlerisiko gegenüber Neuentwicklungen. Darüber hinaus können Unternehmen als Service-Consumer jene Services nutzen, die von Service-Providern bereits angeboten werden. Außerdem reduziert die Mehrfachnutzung von Diensten die Entwicklungs- und Wartungskosten und erleichtert die Wartung. Andererseits können sich Sicherheitslücken in einem Dienst gravierend auswirken, da er von einer Vielzahl anderer genutzt wird.

Nicht verloren gehen darf der Überblick über die vorhandenen Services und deren Eigenschaften. Hierzu ist zweierlei erforderlich: zum einen die Kenntnis der Services und ihrer Schnittstellen und zum anderen die genaue Beschreibung der Services einschließlich ihrer Sicherheitsniveaus je Sicherheitskriterium.

Verzeichnis der Services

Einen Überblick über die Services und ihre Schnittstellen, wie er insbesondere auch zur Laufzeit in Produktion erforderlich ist, liefert beispielsweise eine Registry. Für detailliertere Informationen über die jeweiligen Dienste ist ein Repository notwendig, das die Dienste auch kategorisiert. Es unterstützt primär die Entwicklungsphasen von der Konzeption über die Implementierung bis zur Wartung.

Registries lassen sich durch UDDI (Universal Description, Discovery and Integration), einen Verzeichnisdienst, erstellen. UDDI repräsentiert einen Standard der OASIS™, der Organization for the Ad-vancement of Structured Information Standards. UDDI spezifiziert Protokolle, mit denen sich eine Registry von Web-Services erstellen lässt, ferner Methoden zur Zugriffsregelung sowie einen Mechanismus zur Verteilung oder Delegation von Einträgen an andere Registries. UDDI unterstützt darüber hinaus die digitale Signatur.

SOA
Referenzmodell

Im Oktober 2006 hat OASIS™ das Referenzmodell für eine service-orientierte Architektur in „Reference Model for Service Oriented Architecture“, Version 1.0, verabschiedet. Es stellt ein Rahmenwerk dar und dient dazu, die wesentlichen Entitäten und deren Beziehungen untereinander zu verstehen. Außerdem soll es als Grundlage für die Entwicklung konsistenter Standards oder Spezifikationen für diese Umgebung sowie zur Erklärung und zum Training von SOAs dienen. Architekten können das Referenzmodell verwenden, um service-orientierte Architekturen zu entwickeln.

WSDL

SOA nutzt in der Regel die Standards für Web-Services. Hierbei beschreibt die Web Services Description Language des W3C®, kurz WSDL, die Dienste. Das Simple Object Access Protocol (SOAP) des W3C® spezifiziert den Informationsaustausch zwischen den Diensten.

WSDL spezifiziert in XML die Sprache zur Beschreibung sowohl der abstrakten Funktionalität als auch der konkreten Details von Services. Zur abstrakten Beschreibung gehört die Art der gesendeten und empfangenen Nachrichten sowie deren Reihenfolge. Die Leistungsmerkmale (features) sind ein weiteres Element. Sie enthalten beispielsweise Angaben zur Zuverlässigkeit und Sicherheit des Service. Die Details beziehen sich z. B. auf das konkrete Transportformat für eine oder mehrere Schnittstellen. Das W3C® hat im Mai 2007 die Version 2.0 von WSDL zur abschließenden Freigabe vorgelegt.

SOAP

Das Simple Object Access Protocol (SOAP), Version 1.2, 2. Ausgabe, vom 27. April 2007, ist ein Protokoll des W3C® zum Austausch strukturierter Informationen in einer dezentralen und verteilten Umgebung. Es spezifiziert ein erweiterbares Rahmenwerk zum Nachrichtenaustausch unter Nutzung von XML-Technologien.

Teil 1 der Spezifikation definiert den SOAP-Umschlag (Envelope) und das Rahmenwerk. Der Umschlag setzt sich zusammen aus einem Header und einem Body. Die Nutzlast befindet sich im Body.

Der optionale Header kann Zusatzinformationen enthalten, die nicht zur Nutzlast gehören. Dies können Steuerungsinformationen an einzelne SOAP-Knoten, die sogenannten SOAP-Zwischenstationen

(SOAP-Intermediaries), sein, die sich auf dem Pfad zwischen Sender und Empfänger befinden. SOAP-Zwischenstationen können auf diese Weise angeforderte Zusatzleistungen erbringen, die sich z. B. auf das Routing oder die Verschlüsselung beziehen. SOAP-Knoten können Header prüfen, einfügen, löschen oder weiterleiten.

Die Inhalte von Header und Body hängen zwar von der Applikation ab, jedoch beschreibt SOAP, wie diese zu verarbeiten sind. Das Rahmenwerk spezifiziert die Anbindung von SOAP an darunter liegende Protokolle.

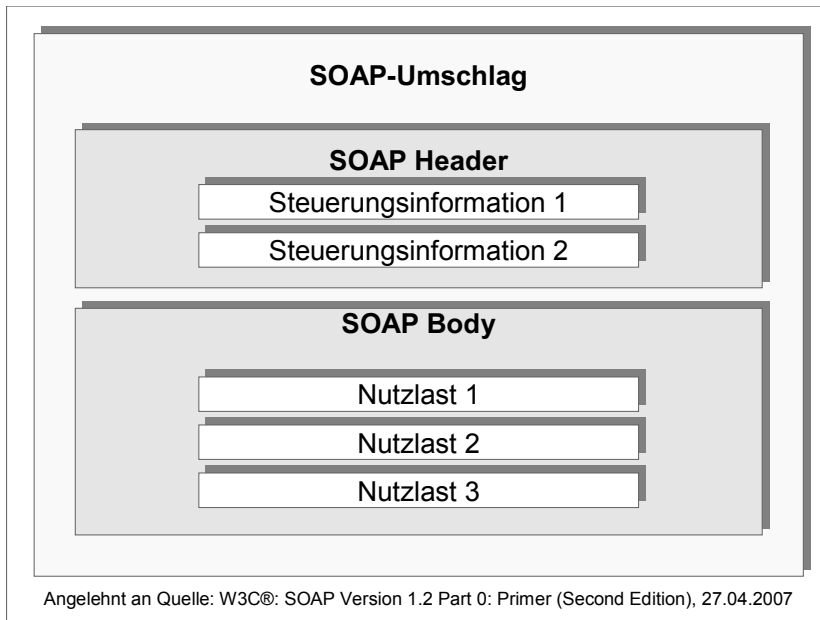


Abb. 9.15: Struktur einer SOAP-Nachricht (Beispiel)

SOAP Teil 2 definiert das Datenmodell für SOAP sowie ein Darstellungsschema für Datentypen. Außerdem konkretisiert er die Anbindung von SOAP an http entsprechend dem Rahmenwerk aus Teil 1.

Das Thema Sicherheit ist eine wesentliche Aufgabestellung im Kontext von SOA. Services sollen die gestellten Anforderungen hinsichtlich Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit erfüllen. Diese Anforderungen müssen die Architekten zu Beginn jeglicher SOA-Überlegungen erheben, um sie dann entlang dem gesamten Lebenszyklus zu berücksichtigen und weiter zu verfeinern.

SOA Security

Darüber hinaus ist zu definieren, welche Sicherheits-Services erforderlich sind. Services müssen sich untereinander authentisieren und authentifizieren und sicherstellen, dass nur berechnigte Service-Nehmer Leistungen erhalten und auch nur die Leistungen, zu denen sie autorisiert sind. Die anforderungsgemäß vertrauliche und integrale Kommunikation ist sicherzustellen.

Services sollen ein zugesichertes Sicherheitsniveau bereit stellen. Hierzu gehört u. a. die Anwendung der Prinzipien des generellen Verbots, der minimalen Rechte, der minimalen Dienste und der Funktionstrennung sowie die Protokollierung (logging) und Protokollauswertung (auditing). Services müssen außerdem im zugesicherten Umfang verfügbar und z. B. gegen DoS-Attacken geschützt sein. Services dürfen nicht „erschlichen“ werden können und die Leistungsabrechnung muss ordnungsgemäß und nachvollziehbar abgewickelt werden.

Im Lebenszyklus von Services von der ersten Idee an bis hin zum Betrieb und zur Außerbetriebnahme sind Sicherheitsaspekte zu berücksichtigen.

Web Services Security

Zum Schutz von Services untereinander und zum Schutz des Nachrichtenaustausch zwischen Services hat OASIS™ die Web Services Security (WSS) entwickelt. Diese beinhaltet SOAP Message Security und verschiedene Token Profiles. In 2007 hat OASIS™ darüber hinaus die Standards WS-Trust und WS-SecureConversation verabschiedet.

WSS SOAP Message Security

WSS SOAP Message Security ist ein OASIS™-Standard, der dem sicheren Austausch von SOAP-Messages zwischen Anwendungen dient. Die Version 1.1 stammt vom 1. Februar 2006. SOAP Message Security ist eine XML-Spezifikation, die einen Standardsatz von SOAP-Erweiterungen definiert. Durch ihn lassen sich Integrität und Vertraulichkeit von Nachrichteninhalten bei der Entwicklung sicherer Web-Services implementieren. Der Standard unterstützt unterschiedliche Security Tokens und Signaturen, verschiedene Verschlüsselungstechnologien sowie E2E-Nachrichtensicherheit, also Nachrichtensicherheit auf der Anwendungsebene, nicht nur auf der Transportebene. Security Tokens beschreiben sicherheitsrelevante Ansprüche bzw. Berechtigungen. Hierfür kann sich ein Dritter, eine Instanz (authority), verbürgen bzw. die Richtigkeit bestätigen.

Folgende Token Profiles sind im Rahmen der WSS SOAP Message Security definiert:

- Username Token Profile,
beschrieben im gleichnamigen OASIS™-Standard, Version 1.1,

vom 1. Februar 2006.

Spezifikation des Username Tokens als Mittel zur Identifikation des Nutzers gegenüber dem Service Provider unter optionaler Verwendung eines Passwortes oder eines gemeinsamen Geheimnisses oder eines Passwort-Equivalents. Zum Schutz vor Replay-Attacken erstreckt sich die Spezifikation auch auf die optionale Nutzung einer Zufallszahl und eines ergänzenden Zeitstempels

- Security Assertion Markup Language (SAML) Token Profile, beschrieben im OASIS™-Standard „SAML Token Profile“, Version 1.1, vom 1. Februar 2006.
Spezifikation von Mechanismen und Prozeduren zur Nutzung von SAML-Assertions als Security Token, insbesondere zur Verifizierung eines Subjekts und seiner Ansprüche
- X.509 Certificate Token Profile, beschrieben im gleichnamigen OASIS™-Standard, Version 1.1 vom 1. Februar 2006.
Spezifikation der Syntax und Verarbeitungsregeln bei der Nutzung von X.509-Zertifikaten, einem ITU-T-Standard für eine Public-Key-Infrastruktur (PKI), einem Standard für digitale Zertifikate. X.509 bezieht sich üblicherweise auf PKIX der IETF
- Kerberos Token Profile, beschrieben im gleichnamigen OASIS™-Standard, Version 1.1 vom 1. Februar 2006.
Spezifikation eines Profils zur Nutzung von Kerberos™, insbesondere zur Verschlüsselung von Kerberos™-Tokens (Service-Tickets und Authentisierungstickets), und deren Einbindung in SOAP Messages, so dass Dienste Tickets authentifizieren und mit bestehenden Kerberos™-Implementierungen zusammenarbeiten können
- Rights Expression Language (REL) Token Profile, beschrieben im gleichnamigen OASIS™-Standard, Version 1.0, vom 19. Dezember 2004.
Spezifikation zur Nutzung der ISO/IEC 21000-5 Rights Expression Language zum Schutz geistigen Eigentums (Intellectual Property), d. h. Urheberrecht.

WS-Trust ist ein OASIS™-Standard, dessen Version 1.3 vom 19. März 2007 stammt. Die Spezifikation dient der Etablierung und Beurteilung sowie dem Management vertrauenswürdiger Beziehungen beim Informationsaustausch zwischen den Beteiligten. Dieses Vertrauen basiert auf dem Austausch und der Vermittlung von Sicherheitstokens. WS-Trust beschreibt das Verfahren zur Ausgabe, Erneuerung und Validierung dieser Tokens. Hierzu spezifiziert der Standard entsprechende Erweiterungen zu WSS.

WS-Trust

WS-Secure- Conversation

WS-SecureConversation ist ein OASIS™-Standard, dessen Version 1.3 vom 1. März 2007 stammt. Der Standard soll die sichere Kommunikation vereinfachen, indem er es Organisationen ermöglicht, mehrere Nachrichten auszutauschen, ohne sich jedes Mal aufwändig erneut gegenseitig authentifizieren zu müssen. Hierzu ermöglicht er den Aufbau eines Sicherheitskontextes zwischen den kommunizierenden Parteien, der für die Dauer einer Sitzung gültig ist.

In Form eines zusätzlichen Token-Typs spezifiziert WS-SecureConversation Erweiterungen der WSS, um einen Sicherheitskontext aufbauen und modifizieren sowie miteinander teilen zu können. Nachdem der Sicherheitskontext aufgebaut ist und ein Geheimnis zwischen den Beteiligten ausgetauscht ist, können die beteiligten Parteien nach spezifizierten Mechanismen sogenannte „abgeleitete Schlüssel“ (derived keys) bilden.

Der Standard empfiehlt, innerhalb der Sitzung statt des Sitzungsschlüssels davon abgeleitete Schlüssel zur Signierung und Verschlüsselung einzusetzen. Beispielsweise können zwei beteiligte Parteien vier Schlüssel ableiten, um jeweils separat signieren und verschlüsseln zu können. Um möglichst wenig Angriffsfläche für Analysen zu bieten, können die Beteiligten weitere Schlüssel ableiten. Je Nachricht geben sie dann an, welchen der Schlüssel sie verwenden.

Zur Bildung abgeleiteter Schlüssel lassen sich unterschiedliche Algorithmen verwenden. Die Spezifikation beschreibt einen Algorithmus. Er nutzt einen Subset jenes Mechanismus, der in RFC 2246 für TLS beschrieben ist, nämlich die P_SHA-1-Funktion. Hiermit lässt sich eine Bytefolge erzeugen, die sich zur Generierung weiterer Schlüssel nutzen lässt.

SAML

Die Security Assertion Markup Language (SAML), eine Auszeichnungssprache für Sicherheitsbestätigungen, ist ein XML-Rahmenwerk zum Austausch von Sicherheitsinformationen zwischen Einheiten, wie z. B. Onlinegeschäftspartnern. Die Version 2.0 dieses Standards hat OASIS™ am 15. März 2005 verabschiedet. SAML beschreibt die Syntax und Verarbeitungsregeln für die Erzeugung und den Austausch von Authentisierungs- und Autorisierungsinformationen.

SAML nutzt zwei Parteien, die bestätigende Partei (asserting party bzw. SAML authority) und die vertrauende Partei (relying party). Die SAML authority ist ein System, das Informationen über ein Subjekt bestätigt. Die SAML authority sichert beispielsweise zu, dass sie ein Subjekt, z. B. einen Benutzer, erfolgreich authentifiziert hat, dass sie das Subjekt mittels Passwort authentifiziert hat und dass das Subjekt bestimmte Attribute, wie z. B. die angegebene E-Mail-Adresse besitzt.

Die relying party ist ein System, das sich auf die Zusicherungen der SAML authority verlässt. Das lokale System bestimmt selbst, auf welche Ressourcen es das so identifizierte Subjekt zugreifen lässt.

SAML 2.0 berücksichtigt Anforderungen der Liberty Alliance aus dem Liberty Identity Federation Framework ID-FF V1.2. Der funktionale Ansatz von SAML 2.0 ist hierbei gleichwertig, wird jedoch strukturell auf anderem Wege umgesetzt. Zusätzlich hat SAML 2.0 die Liberty-Funktionalitäten für mehr Anwendungsfälle verallgemeinert. Die Version 2.0 von Liberty's Identity Web Services Framework (ID-WSF) nutzt SAML 2.0 Assertions als Format für Sicherheitstoken, die Authentisierungs- und Autorisierungsinformationen zwischen Web Services austauschen.

SAML spezifiziert Assertions, Protokolle, Bindings und Profile. Assertions (Ansprüche, Rechte) beinhalten Informationen zur Authentifizierung und zu Attributen. Eine Assertion enthält drei Arten von Informationen: das Authentication Statement, das Attribute Statement und das Authorization Decision Statement. Das Authentication Statement enthält die Authentifizierung ein Subjekts, wobei es Authentifizierungsart und -zeit angibt. Dieses Statement erzeugt üblicherweise eine SAML authority, ein sogenannter Identitäts-Provider, dessen Aufgabe darin besteht, Nutzer zu identifizieren und diesbezügliche Informationen bereit zu stellen. Das Attribute Statement enthält Details, die dem Subjekt zugeordnet sind, wie z. B. Mitgliedschaft, Status oder E-Mail-Adresse. Das Authorization Decision Statement schließlich enthält die Entscheidung einer Autorisierungsinstanz, ob und wenn ja, wozu ein Subjekt berechtigt ist, z. B. ob und wie es auf eine spezifische Ressource zugreifen darf.

Protokolle ermöglichen es, SAML-Assertions mittels einer Anfrage anzufordern und in Form einer Antwort zu übermitteln. Dadurch können Service Provider einen Identity-Provider auffordern, z. B. einen Nutzer zu authentifizieren und die dazu gehörigen Assertions zu übermitteln, ein annähernd simultanes Logout („single logout“) mehrerer Sitzungen durchzuführen, eine Namenskennung zu registrieren oder deren Nutzung zu beenden.

Bindings legen im Detail fest, wie SAML Anfragen und Antworten in Standard-Transport- und -Nachrichten-Protokolle einzubinden sind, z. B. in den SOAP Body einer SOAP Message über http.

Profile schließlich ermöglichen es, Assertions, Protokolle und Bindings für spezielle Anwendungsfälle einzuschränken, zu erweitern und zusammenzustellen. So lässt sich beispielsweise ein Single-Sign-on-Profil für einen Web-Browser spezifizieren, das angibt, wie ein

Identity-Provider und ein Service-Provider SAML-Authentifizierungs-Assertions austauschen, um einem Browser-Nutzer ein Single Sign-on zu ermöglichen.

XACML

Die eXtensible Access Control Markup Language (XACML) ist ein OASISTM-Standard, der in der Version 2.0 im Februar 2005 verabschiedet wurde. XACML beschreibt sowohl ein XML-Schema für die „security policy“ als auch eins zur Anfrage nach einer Zugriffs-erlaubnis und deren Beantwortung. Wer beispielsweise auf eine Resource, z. B. einen Web-Service, zugreifen möchte, richtet eine Anfrage an das System, das diese Ressource schützt, z. B. einen Web-Server oder ein Dateisystem. XACML bezeichnet das schützende Systeme als Policy Enforcement Point, kurz PEP. Der PEP seinerseits richtet die Anfrage mit den Attributen des Benutzers, der angefragten Resource und der gewünschten Berechtigung sowie weiteren Informationen an den Policy Decision Point (PDP). Dieser prüft die Anfrage und antwortet, ob der Zugriff erlaubt werden kann. Auf Basis dieser Information gewährt der PEP den Zugriff oder lehnt ihn ab.

XML Security Framework

Das XML Security Framework des World Wide Web Konsortiums (W3C[®]) für die Sicherheit von Web-Applikationen besteht aus folgenden Komponenten:

- XML Key Management System (XKMS)
- XML Signature Syntax and Processing (XML-Sig)
- XML Encryption Syntax and Processing (XML-Enc) sowie
- Exclusive XML Canonicalization.

XKMS

XML Key Management Specification (XKMS) ist eine Empfehlung (Recommendation) des World Wide Web Consortiums (W3C[®]). Das W3C[®] verabschiedete XKMS in der Version 2.0 am 28. Juni 2005. XKMS besteht aus der XML Key Information Service Specification (X-KISS) und der XML Key Registration Service Specification (X-KRSS). XKMS spezifiziert die Protokolle zur Registrierung und Verteilung von Public Key Informationen. Die Nutzung des XKMS-Service entkoppelt die Anwendung von der Komplexität und der Syntax der zugrunde liegenden Public-Key-Infrastruktur (PKI).

X-KISS

Die XML Key Information Service Specification (X-KISS) definiert Protokolle, die es einem Client-Rechner ermöglichen, alle oder einen Teil jener Aufgaben an einen XKMS-Service zu delegieren, die zur Verarbeitung von XML-Signatur- oder XML-Verschlüsselungselementen erforderlich sind. Wesentliches Ziel des Protokoll-Designs ist die Minimierung der Komplexität von Anwendungen, die XML Signature nutzen wollen.

Die XML Key Registration Service Specification (X-KRSS) beschreibt das Protokoll zur Registrierung und zum anschließenden Management von Public Key Informationen. *X-KRSS*

XML Signature Syntax and Processing (XML-Sig) enthält die Spezifikation der Syntax und der Verarbeitungsregeln für eine digitale XML Signatur (XML digital signature). Enthalten sind Services im Hinblick auf die Integrität sowie Services zur Authentifizierung von Nachrichten und/oder Unterzeichnern. *XML-Sig*

XML Encryption Syntax and Processing (XML-Enc) spezifiziert den Verschlüsselungsprozess beliebiger Daten, die Ergebnisdarstellung als XML Encryption Element, das den Kodierschlüssel enthält oder referenziert, sowie die Syntax des XML Encryption Elements. *XML-Enc*

Exclusive XML Canonicalization ermöglicht den Ausschluss des Vorgänger-Kontexts eines kanonischen (normalisierten) Unterdokuments. Kanonisches XML beschreibt die Serialisierung von XML, bei der das Einfügen eines Unterdokuments dessen Vorgänger-Kontext mit übernimmt einschließlich der Namespace-Deklarationen und Attribute. Beim Transport der digitalen Signatur als Unterdokument in einer XML-Nachricht soll das Entfernen der Signatur die Nachricht jedoch nicht zerstören. Dies ermöglicht die exklusive XML Kanonisierung.

Digital Signature Services (DSS) ist ein Standard, den die OASIS™ als „Digital Signature Service Core Protocols, Elements, and Bindings“ in der Version 1.0 im April 2007 verabschiedet hat. Er nutzt XML und spezifiziert damit zwei Frage-Antwort-Protokolle für Services, die der Signierung von Dokumenten bzw. der Verifizierung von Signaturen durch einen Servicegeber dienen. Bei der Signierung schickt ein Client Dokumente bzw. deren Hashwerte an einen entsprechenden Server und bekommt sie unterschrieben zurück. Bei der Verifizierung schickt der Client Dokumente bzw. deren Hashwerte zusammen mit einer Signatur an einen Server und lässt die Signatur überprüfen. *Digital Signature Services*

Für unterschiedliche Anwendungsfälle existieren spezifische Profile, z. B.

- zur Erzeugung und Verifizierung von Zeitstempeln (time stamps), beschrieben im OASIS™-Standard „XML Timestamping Profile of the OASIS Digital Signature Services“, Version 1.0, vom 11. April 2007
- zur Erzeugung und Validierung elektronischer Signaturen, beschrieben im OASIS™-Standard „Advanced Electronic Signature Profiles of the OASIS Digital Signature Service“, Version 1.0, vom 11. April 2007.

Der Standard bezieht sich auf elektronische Signaturen, die in

„XML Advanced Electronic Signatures“ (XAdES) sowie in „CMS-based Advanced Electronic Signatures“ (CAdES) des W3C® definiert sind

- zur Code-Signierung, beschrieben im OASIS™-Standard „Abstract Code-Signing Profile of the OASIS Digital Signature Services“, Version 1.0, vom 11. April 2007.
Der Standard spezifiziert die digitale Signierung von Software-Programmen in Form von Quellcode oder in kompilierter Form
- zur Erzeugung und Validierung qualifizierter Signaturen gemäß den Richtlinien des deutschen Signaturgesetzes (SigG) und der Signaturverordnung (SigV), beschrieben im OASIS™-Standard „German Signature Law Profile of the OASIS Digital Signature Service“, Version 1.0, vom 11. April 2007.
Der EU zufolge entspricht das deutsche Signaturgesetz den gesetzlichen Vorgaben der EU. Dieses Profil kann daher europaweit als Vorlage für andere nationale Profile dienen
- zum elektronischen Abstempeln von Post (Postmarking), beschrieben im OASIS™-Standard „Electronic PostMark (EPM) Profile of the OASIS Digital Signature Service“, Version 1.0, vom 11. April 2007.
Der Standard spezifiziert Dienste zur Erzeugung und Verifizierung digitaler Signaturen, zum Zeitstempeln, zum Quittieren und zur nachweisbaren Aufzeichnung. Diese Dienste sind nutzbar von und zwischen Postverwaltungen und ihren Kunden.

*Application
Vulnerability
Description
Language*

Die Application Vulnerability Description Language (AVDL) ist ein OASIS™-Standard, beschrieben in „Application Vulnerability Description Language“, Version 1.0 vom Mai 2004. Er legt ein einheitliches Format fest, mit dem sicherheitsrelevante Schwachstellen von Anwendungen in XML beschrieben und dadurch diesbezügliche Informationen in einheitlichem Format ausgetauscht werden können. AVDL konzentriert sich auf Schwachstellen beim Nachrichtenaustausch über http-Protokolle auf der Anwendungsschicht und zwar zwischen Clients und Gateways auf der einen und Internetsystemen sowie Hosts auf der anderen Seite.

*Common
Alerting
Protocol*

Das Common Alerting Protocol (CAP) ist ein OASIS™-Standard, beschrieben im „Common Alerting Protocol“, Version 1.1, vom Oktober 2005. Er beschreibt ein allgemeines XML-Format zum Austausch von Alarmen und öffentlichen Warnungen über alle Arten von Netzen, das unabhängig ist von Anwendungen und Kommunikationsmethoden. Es unterstützt multilinguale und an verschiedene

Zielgruppen gerichtete Nachrichten sowie Verschlüsselung und digitale Signatur.

Die „Emergency Data Exchange Language – Distribution Element“ (EDXL-DE), Version 1.0, vom März 2006 ist ein OASIS™-Standard. Er beschreibt eine XML-basierte Sprache, mit der sich Notfalldaten in standardisierter Form über beliebige Übertragungsmedien, u. a. über SOAP und http, austauschen lassen. Er dient dazu, Notfallnachrichten, z. B. Alarmer und Meldungen von Ressourcen zu verteilen, indem Routing-Informationen mitgegeben werden. Diese betreffen z. B. den Nachrichtentyp, wie Alarm, Aktualisierung, Bestätigung, Storno oder Fehler, das betroffene Zielgebiet, das Ereignis und die Sender/Empfänger-ID. Ziel ist die gemeinsame Nutzung von Notfallinformationen und deren Austausch zwischen lokalen, staatlichen, nationalen und Nicht-Regierungsorganisationen, insbesondere dann, wenn mehr als eine Berufsgruppe beteiligt ist.

*Emergency
Data Exchange
Language*

9.5.19.2 Grid-Computing

Beim Grid-Computing sind verschiedene Computer so vernetzt, dass sie gleichzeitig an der Lösung einer Aufgabe arbeiten können. Die Computer stellen dabei die „Knotenpunkte“ des „Gitters“ dar. Die Nutzer können auf die Rechenkapazität aller im Netz angeschlossenen Geräte zugreifen. Hierdurch lassen sich Geschäftsprozesse beschleunigen, rechenintensive Simulationen durchführen und die Rechnerauslastung optimieren. Wegen der großen Zahl vernetzter Rechner und der Vielzahl unterschiedlich lokalisierter Nutzer muss für alle Sicherheitskriterien auf Sicherheitsaspekte besonderer Wert gelegt werden.

*Grid-
Computing*

Ähnlich wie bei SOA betrifft dies u. a. die sichere Identifikation und Authentisierung der beteiligten Systeme untereinander, den sicheren verschlüsselten Datenaustausch und die Verbindungsüberwachung. Auf den Grid-Knoten ist das geforderte Sicherheitsniveau sicherzustellen. Hierzu gehört u. a. die Anwendung der Prinzipien des generellen Verbots, der minimalen Rechte, der minimalen Dienste und der Funktionstrennung sowie die Protokollierung (logging) und Protokollauswertung (auditing). Der Lebenszyklus von Grids und ihren Komponenten spielt ebenfalls eine wesentliche Rolle. Von der ersten Idee an bis hin zum Betrieb und zur Außerbetriebnahme sind Sicherheitsaspekte zu berücksichtigen. Die Phasen des Hinzuschaltens, Ausklinkens und Abschaltens einzelner Komponenten müssen ebenfalls unter Sicherheitsaspekten betrachtet werden.

Open Grid Forum

Mit dem Thema Grid hinsichtlich Standards und Best Practices einschließlich Security beschäftigt sich das „Open Grid ForumSM“ (OGFSM). Im Juni 2006 gaben die „Enterprise Grid Alliance“ (EGA) und das „Global Grid Forum“ (GGF) bekannt, dass sie das OGF gegründet haben. Das GGF hatte sich zuvor auf Basis des Grid ForumsSM, das 1998 gegründet worden war, im Jahr 2000 mit dem European Grid Forum (eGrid) und dem Asia Pacific Grid Forum vereint. Die EGA war im April 2004 gegründet worden. Die EGA veröffentlichte u. a. das EGA Reference Model und Use Cases. Außerdem stellte sie Anforderungen an die Security zusammen.

Open Grid Services ArchitectureTM

The Open Grid Services ArchitectureTM (OGSATM), Version 1.5, vom 24. Juli 2006, des OGF dient dazu, die Nutzung und das Management verteilter heterogener Ressourcen zu vereinfachen. OGSATM enthält Dienste, Schnittstellen, den Status von Ressourcen sowie die Interaktion zwischen den Diensten in einer SOA. Ferner spricht das Dokument das Thema Sicherheit an. Die Dienste bauen hierbei auf Standards für Web Services auf, die im Hinblick auf grid-relevante Aspekte erweitert oder verändert werden.

Grid Security

Die dortigen Autoren des Dokuments führen zum Thema Security aus, dass zur sicheren Administration der Zugriff auf die Services durch robuste Sicherheitsprotokolle und gemäß einer entsprechenden Sicherheitsrichtlinie (security policy) zu steuern ist. Die dort genannten Sicherheitsanforderungen umfassen:

- Authentisierung und Autorisierung von Individuen und Diensten
- Integration und Interoperabilität unterschiedlicher Sicherheitsinfrastrukturen in Form von Architekturen und Modellen
- Sicherheitslösungen an den Schnittstellen bei unternehmensübergreifender Zusammenarbeit, z. B. in Form einer firewall policy und einer intrusion detection policy
- Kapselung, beispielsweise von Nutzern
- Delegation von Zugriffsrechten von Dienstanfordernden (Service Requestor) auf Diensteanbieter (Service Provider) sowie der Schutz vor Missbrauch
- Austausch von Sicherheitsrichtlinien (security policies) zwischen Dienstanfordernden und Diensteanbietern
- Intrusion detection und protection sowie sichere Protokollierung.

Das OGSATM Basic Security Profile 1.0 – Core vom 10. November 2006 lässt sich dazu nutzen, eine sichere Kommunikation mit einem Web-Service aufzubauen. Das OGSATM Security Profile 1.0 – Secure Channel vom 22. Januar 2007 beschreibt ein sicheres Trans-

port-Layer-Protokoll mit gegenseitigen Authentisierungs-, Integritäts- und Vertraulichkeitsattributen. Es dient dem sicheren und interoperablen Zusammenspiel von Web Services im Umfeld verteilter Ressourcen und beim Grid-Computing.

Die Spezifikation „Use of SAML for OGSi Authorization“ des OGF vom 26. März 2006 definiert einen Autorisierungsdienst für die Open Grid Services Infrastructure (OGSI). Sie befindet sich im Status „experimentell“ und basiert auf SAML.

In der Security Policy Assertion Language (SecPAL) Specification [51], Version 1.0, vom 15. Februar 2007 hat Microsoft® eine deklarative Sprache für Security Policies entwickelt. Sie ist ausgerichtet auf die Zugriffsschutzanforderungen großer Grid-Computing-Umgebungen (Grid Computing Environment {GCE}) und basiert auf XML.

9.5.20 Innovationsmanagement (Innovation Management)

**Wer immer strebend sich bemüht,
den können wir erlösen.**
(Goethe, Faust II)

Umfelder, Märkte, Technologien und Bedrohungen verändern sich kontinuierlich und haben Auswirkungen auf Kern-, Support- und Begleitprozesse. Innovationen und ihre Auswirkungen rechtzeitig zu erkennen, das Für und Wider abzuwägen, Maßnahmen zu ergreifen und diese umzusetzen ist Aufgabe des Prozesses Innovationsmanagement. An welchen Beispielen aus naher Vergangenheit zeigt sich die Aufgabe des Innovationsmanagements?

Nehmen wir die Einführung der USB-Schnittstelle. Ihre sicherheitsspezifische Bewertung zeigt, dass durch USB-Schnittstellen einerseits neue Bedrohungen entstehen, beispielsweise indem hierüber Schadprogramme und unlicenzierte Programme eingespielt werden können. Auch das unzulässige Kopieren von Daten, noch dazu in großen Mengen, stellt eine Bedrohung dar. Sie wird zusätzlich dadurch unterstützt, dass USB-Sticks teilweise kaum mehr als solche erkennbar sind, wenn sie beispielsweise in ein Schweizer Taschenmesser oder eine Armbanduhr integriert sind. Andererseits eröffnet die USB-Schnittstelle die Möglichkeit, große Datenmengen einfach und leicht zu transportieren bis hin zum multi-bootfähigen USB-Stick mit Betriebssystemen, Anwendungen und Daten oder der Möglichkeit, USB-Tokens, auch biometrische, zum Sign-on zu nutzen.

*Innovations-
beispiel*

Weitere
Beispiele
für
Innovationen

Sowohl Chancen als auch Risiken zeigt die Sicherheitsbetrachtung neuerer Technologien in Form mobiler Geräte, wie z. B. Notebooks, PDAs und Handys, sowie der drahtlosen Übertragung über Bluetooth und WLANs.

Unternehmen setzen zunehmend biometrische Verfahren ein. Verschiedene biometrische Verfahren für den Zutrittsschutz zum Gebäude und zu Hochsicherheitsbereichen bieten Vorteile, aber auch Risiken, z. B. durch Falscherkennung. Dies gilt auch für den Zugangsschutz mittels Fingerabdruck-Sensoren, z. B. zum Unternehmensnetz und zur Unternehmens-IT, zu Notebooks, zu USB-Memory-Sticks und zu mobilen Festplatten. Chancen-Risiken-Abwägungen sind auch erforderlich für die Stimmerkennung beim Telefon-Banking und für den Self-Service zur Passwort-Rücksetzung. Das Bezahlen per Fingerabdruck bietet Handelsunternehmen die Vorteile schnellerer Bezahlvorgänge, höherer Transaktionsraten und geringerer Kosten sowie den Kunden höheren Komfort. Doch auch hier sind Sicherheitsaspekte zu berücksichtigen.

Gleiches gilt für die vom Marktforschungsunternehmen IDC unter dem Begriff Unified Threat Management (UTM) identifizierten Appliances, die in sich die Funktionalitäten von Firewall, Intrusion Detection and Prevention sowie Virenschutz vereinigen, aber auch für technologische Fortschritte bei Standards und Werkzeugen zur Überwachung von Service-Levels und Ende-zu-Ende-(E2E-)Verfügbarkeit etc.

Ein weiteres aktuelles Thema im Innovationsmanagement ist die Bewertung des Single Sign-on sowie des Identitäts- und Access-managements, das auch unter Wirtschaftlichkeitsaspekten interessant sein kann. Das föderierte Identitätsmanagement eröffnet darüber hinaus neue Geschäftsmöglichkeiten.

Wegen der zunehmenden Nutzung von Netzwerkdruckern bieten deren Hersteller Lösungen an, bei denen die Ausgabe eines Druckjobs erst dann erfolgt, wenn der berechtigte Benutzer diesen am Drucker initiiert. Zur Auslösung stehen Verfahren mit PINs und Magnet- oder Chipkarten, aber auch biometrische Verfahren zur Verfügung.

Das Thema Verschlüsselung gewinnt an Bedeutung. Zunehmend bieten Hersteller Tools zur verschlüsselten Speicherung und Übertragung von Daten sowohl bei Computern als auch peripheren Einheiten, wie Druckern und Speichermedien bis hin zu USB-Sticks und Bändern an.

Service orientierte Architekturen und Grids sind aktuelle Themenstellungen für Organisationen und Unternehmen. Deren Sicherheit und Verfügbarkeit bzw. Kontinuität sind im Sicherheits- und Konti-

nitätsmanagement unter Berücksichtigung aktueller Standards zu beachten.

Für das Internet, das als kritische Infrastruktur zu sehen ist, baut das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen ein Security-Frühwarnsystem auf, um das Internet sicherer zu machen. Hierbei soll das Internet-Analyse-System (IAS) einen Überblick über den aktuellen Zustand des Internets liefern, Angriffe erkennen und Prognosen von Angriffen erstellen. Die hierzu erforderlichen Daten sollen 100–200 passive Sonden liefern, die an ausgewählten Stellen des Internets positioniert sind.

Das Internet-Verfügbarkeits-System nutzt demgegenüber aktive Sonden, die Dronen. Sie messen die Verfügbarkeit von Ressourcen, wie z. B. Kommunikationsverbindungen und Routern, sowie Diensten, z. B. Web-, DNS- und E-Mail-Diensten, einschließlich der Dienstgüte. Parameter sind hierbei die Fehlerrate, Verzögerungen und Paketverluste.

Bei Bedrohungen zeigen sich ebenfalls „Innovationen“, wie die Spam-Welle, das Phishing und Spyware zeigten und zeigen.

Innovationsmanagement im Hinblick auf IT-Sicherheit und Kontinuität, 2005 in „IT-Sicherheit mit System“ und im „Handbuch Unternehmenssicherheit“ dargestellt, stellt ein wichtiges Element jedes Unternehmens und seiner IT dar. Dies zeigte sich auch im Titel „Innovationsmotor IT-Sicherheit“ des 10. BSI-Kongresses im Mai 2007.

9.5.21 Personalmanagement (Human Resources Management)

Für die Planung, die Entwicklung und den Betrieb der ITK sowie ihres Umfelds sind Personen notwendig. Für diese gilt es, Anforderungsprofile zu erstellen und zu pflegen sowie einen Abgleich zwischen Soll und Ist durchzuführen. Im Personalprozess ist daher die Qualifikation zu prüfen und den Anforderungen entsprechend fortzuentwickeln. Für die Aufgaben der Personen sind – dem Redundanzprinzip folgend – Stellvertreter einzuplanen.

Um Bedienungsfehler und „menschliches Versagen“ präventiv zu vermeiden, sollte auf die Benutzerfreundlichkeit der Informations- und Kommunikationssysteme Wert gelegt und das Poka-Yoke-Prinzip angewendet werden.

Hieraus ergeben sich die folgenden Sicherheitselemente:

- sicherheitskonformer Personalprozess
- angemessene und dokumentierte Qualifikation der Mitarbeiter
- benutzerfreundliche Ressourcen, z. B. IT-Anwendungen.

Qualifikation

*Benutzer-
freundlichkeit*

*Sicherheits-
elemente
Personal*

Im Hinblick auf die Sicherheit des Unternehmens stellen die Menschen, d. h. die Mitarbeiter und Mitarbeiterinnen, einen wesentlichen Faktor dar. Daher kommt dem Personalprozess eine hohe Bedeutung zu. Für die Phasen des Personalprozesses muss die Sicherheitsarchitektur geeignete Sicherheitselemente enthalten. Der Personalprozess umfasst folgende Phasen:

- Planung
- Beschaffung (Recruiting)
- Einarbeitung
- Betreuung und Weiterentwicklung
- Trennung.

Planungsphase

In der Planungsphase definiert der Personalverantwortliche, welche neu einzustellenden Personen welche Aufgaben wahrnehmen sollen, inwieweit diese sicherheitsrelevant sind, welcher Sicherheitsstufe sie angehören sowie welches Know-how auch im Hinblick auf Sicherheit gefordert ist. Dies dokumentiert er im Skill-Profil, z. B. für einen CISO, CBCO, CCO, Administrator, Datenschutzbeauftragten, Softwareentwickler etc. Darüber hinaus legt er fest, ob es sich um einen befristeten oder unbefristeten Arbeitsvertrag handeln soll.

Beschaffungsphase

In der Beschaffungsphase erfolgt die Auswahl anhand der vorgegebenen Anforderungen. Je nach Sicherheitsstufe führt der Bereich Personal unterschiedliche Sicherheitsprüfungen durch. Diese können sich auf die Anforderung eines polizeilichen Führungszeugnisses sowie die Einholung von Referenzen und Bankauskünften beziehen, oder nur auf die Prüfung, dass der Lebenslauf keine kritischen Lücken aufweist.

Für unternehmens- oder sicherheitskritische sowie betrugsanfällige Aufgaben, wie Buchhaltung, Systemadministration oder Beschaffung, lässt sich die forensische Psychologie zu Integritätstests des Bewerbers nutzen. Persönliche Integrität beinhaltet die Vertrauenswürdigkeit und Aufrichtigkeit einer Person. Ein solcher Test ermittelt z. B. die Anfälligkeit für Korruption und Betrug.

Je nach Aufgabe und Sicherheitsstufe sind familiäre oder enge verwandtschaftliche Beziehungen zwischen dem neu eingestellten Mitarbeiter und vorhandenen Mitarbeitern zu prüfen, um Interessenkonflikte präventiv zu vermeiden. Soll beispielsweise ein Revisor eingestellt werden, so kann es zu Interessenkonflikten kommen, wenn ein Familienangehöriger, z. B. die Gattin, für den Bereich zuständig ist, den er später prüfend begleiten soll.

Kommt es zum Abschluss eines Arbeitsvertrags, so können hiermit beispielsweise die Verpflichtung zur Einhaltung des Bundesdatenschutzgesetzes, der Geheimhaltung von Betriebsgeheimnissen, der Einhaltung des Sozialdatenschutzes und des Bankgeheimnisses – auch über das Vertragsende hinaus – einhergehen.

Während der Einarbeitung stellt ein strukturierter Einarbeitungsplan sicher, dass der neue Mitarbeiter alle erforderlichen Informationen erhält, um die Aufgaben nach der Einarbeitung fehlerfrei wahrnehmen zu können. Im Hinblick auf die Sicherheit gehören hierzu allgemeine Informationen, z. B. über die Sicherheits-, Kontinuitäts- und Risikopolitik sowie Sicherheitsrichtlinien wie das „Verhalten in Notfällen“, der Räumungsplan, „Sicherheitsbewusstes Verhalten“, die IT-Benutzerordnung sowie Regelungen zur E-Mail- und Internet-Nutzung. Die Sicherheits-, Kontinuitäts- und Risikopolitik gibt hierbei den normativen Rahmen vor, den alle Mitarbeiter einzuhalten haben, insbesondere auch bei der Erreichung individuell vereinbarter Ziele.

*Einarbeitungs-
phase*

Außerdem erhält der neue Mitarbeiter spezifische sicherheitsrelevante Informationen, welche seine jeweilige Aufgabenstellung und seine Verantwortlichkeiten betreffen. Diese Informationen können in Form von Unterlagen und/oder über Schulung oder Patenschaften vermittelt werden. Schulungen sollten spezifisch auf die Aufgabenstellung und das vorhandene Grundwissen der Zielgruppe abgestimmt sein.

Die Phase der Betreuung und Weiterentwicklung soll erreichen, dass die Führungskraft rechtzeitig sicherheitsrelevante Entwicklungen, wie z. B. finanzielle, familiäre oder persönliche Schwierigkeiten des Mitarbeiters, erkennt. Primäres Ziel muss es sein, frühzeitig Unterstützung anbieten zu können, um Fehlentwicklungen zu vermeiden. Grundlage hierfür ist eine geeignete Unternehmenskultur, gekennzeichnet durch Fairness und Offenheit auch in schwierigen Zeiten. Bewährt haben sich Methoden des „management by walking around“ und die „open door policy“.

*Betreuungs-
und Weiter-
entwicklungs-
phase*

Auch im Sicherheitsbereich sind an vielen Stellen die vier Dimensionen fachliche, methodische, soziale und persönliche Kompetenz gefordert. Zu den Aufgaben einer Führungskraft gehört es, die Qualifikationsprofile der Mitarbeiter mit den aktuell und mittelfristig geforderten in Einklang zu halten. Dies erfordert die Vereinbarung, Planung, Durchführung und Erfolgsbewertung von Qualifikationsmaßnahmen. Führungskräfte können so die Qualifikationen kontinuierlich steuern. Der Abgleich zwischen Soll und Ist bildet letztendlich ein Element einer „lernenden“ Organisation. Für das Thema dieses

Buchs handelt es sich also um ein Element einer „lernenden“ Sicherheits-, Kontinuitäts- und Risikoorganisation.

Damit Mitarbeiter möglichst fehlerfrei arbeiten und im Hinblick auf sicherheitsrelevante Entwicklungen im eigenen Aufgabengebiet auf dem Laufenden sind, sollten regelmäßig zielgruppenspezifische Fortbildungen stattfinden. Darüber hinaus sollten Mitarbeiter regelmäßig zum Thema Sicherheit sensibilisiert und damit das Sicherheitsbewusstsein (awareness) gestärkt werden. Als Medien zur Sensibilisierung kommen z. B. Quiz, Rätsel, Newsletter, Bilder, Videos, Ausstellungen, Rundgänge, Workshops, Informationsportale und Kommunikationsforen in Betracht. „Fiktive“ Angriffe können sensibilisieren. Deren Auswertung hilft bei der Risikoeinschätzung. Die darauf folgende gezielte und abgestufte Ansprache unzureichend sensibler Mitarbeiter erhöht deren Sicherheitsbewusstsein. Die Sensibilisierung der Management-Ebene erfolgt z. B. durch das Berichtswesen, wie es im Sicherheitsregelkreis beschrieben ist.

Bei der Führungsmethode „Management by Objectives“ (MbO) kann die Führungskraft mit dem Mitarbeiter Ziele auch zum Thema Sicherheit vereinbaren und durch ein entsprechend gestaltetes Anreizsystem den Willen zur Zielerreichung unterstützen.

*Trennungs-
phase*

Für die Phase der Trennung von einem Mitarbeiter sollte es ein Standardverfahren geben. Dieses definiert, wer auf welcher Basis die Entscheidung trifft, ob ein Mitarbeiter freigestellt wird oder nicht und welche Berechtigungen ihm für die verbleibende Unternehmenszugehörigkeit zugewillt werden. Weiterhin muss das Verfahren sicherstellen, dass betriebsrelevante Unterlagen und Dateien, aber auch Geräte zurückgegeben wurden. Der Ablauf ist so zu gestalten, dass auch alle Berechtigungen dieses Mitarbeiters spätestens zum Zeitpunkt des Ausscheidens, genauer direkt am Ende seines letzten Arbeitstages, gesperrt werden.

*Personal ohne
direkte
Zugehörigkeit
zum
betrachteten
Unternehmen*

Der bisherige Prozess des Personalmanagements konzentrierte sich auf interne Mitarbeiter des Unternehmens. Darüber hinaus umfasst er Verfahren, die sich auf Personal ohne direkte Zugehörigkeit zum betrachteten Unternehmen beziehen. Hierzu gehören beispielsweise:

- Handelsvertreter
- Dienstleister mit Werk- oder Dienstleistungsvertrag
 - Berater
 - Wachpersonal
 - Reinigungspersonal
 - Wartungspersonal

- Handwerker
- ...
- Mitarbeiter aus
 - Schwesterunternehmen
 - Holding
 - ...

9.5.22 Ressourcen im Überblick

Die vorangegangenen Kapitel betrachteten die verschiedenen Prozesse der Sicherheitsarchitektur. Die folgenden Kapitel widmen sich den sicherheitsrelevanten Ressourcen. Diese schließen Dokumentationen, Verfahren, Methoden, Werkzeuge und Technik im Sinne von Hardware und Software sowie Infrastruktur, wie z. B. Gebäudetechnik, aber nicht zuletzt auch das Personal ein. Während spezifische Charakteristika der Ressourcen, z. B. technische Daten, in separaten Dokumenten enthalten sind, gibt die Architektur einen Überblick, der das Zusammenspiel bzw. die überblicksartigen Zusammenhänge darstellt. Für jede Schutzobjektklasse sollte die dazugehörige Architektur verfügbar sein.

9.5.23 ITK-Hard- und Software

Ausgangspunkt für die sicherheitsrelevanten Hard- und Softwarekomponenten ist die ITK-Architektur [52] des Unternehmens. In ihr sind die im Unternehmen eingesetzten und für die Zukunft geplanten Hard- und Softwarekomponenten angegeben. Hierzu gehören beispielsweise:

- Rechnerplattformen
- Betriebssysteme
- Datenbanken
- Transaktionsmonitore
- Kommunikationsdienste
- Groupware
- Standardsoftware
- unternehmensspezifische Informationssysteme.

Die Plattform-, die System- und die Anwendungsarchitektur sowie die Netztopologie zeigen das prinzipielle Zusammenspiel und die Verbindungen zwischen den Architekturkomponenten.

In der Sicherheitsarchitektur führen der Sicherheitsbeauftragte und der zuständige ITK-Architekt die Sicherheitskomponenten der Rechnerplattformen und der Softwarekomponenten auf, wie z. B. das jeweilige Rechtesteuerungs- und -verwaltungssystem, das Auditing-tool, das Datensicherungstool etc.

Wer den Hard- und Softwarekomponenten die vorhandenen Sicherheitskomponenten gegenüberstellt, kann Defizite und das Maß der Heterogenität erkennen. Ferner lässt sich kennzeichnen, wie gut die jeweiligen Sicherheitskomponenten die Anforderungen des Unternehmens erfüllen.

Die nächsten Unterkapitel behandeln die folgenden Sicherheitskomponenten etwas detaillierter:

1. Speicher
2. Firewall
3. Intrusion-Detection-, -Response- und -Prevention-System
4. Content-Security-System
5. Computerviren-Suchprogramme
6. Security Appliances
7. Automatisierte biometrische Systeme.

9.5.23.1 Speicher

Speicher lassen sich nach folgenden Kategorien unterscheiden:

- Speicherhierarchie
- Speichermedien
- Speichertopologie.

9.5.23.1.1 Speicherhierarchie

*Speicher-
hierarchie*

Die Speicherhierarchie lässt sich entsprechend den Aufgabenstellungen Echtzeit-Speicherung, Datensicherung oder Archivierung in Primärspeicher, Sekundärspeicher und Tertiärspeicher unterteilen. Primärspeicher sind jene Speichermedien, die für den direkten Datenzugriff in Echtzeit (realtime) genutzt werden. Sekundärspeicher werden zur Datensicherung (Backup) verwendet, während Tertiärspeicher der Archivierung dienen.

Datensicherung

Für die Sekundär- und Tertiärspeicher müssen entsprechende Datensicherungs- und Archivierungsstrategien entwickelt werden. Für die Datensicherung ist hierbei festzulegen, welche Daten in welchem Umfang und Rhythmus wann auf welchem Medium gesichert werden. Die Auswahl des Mediums wird maßgeblich mit bestimmt von

den maximal tolerierbaren Ausfallzeiten. Hierbei müssen die gegenläufig korrelierenden Parameter Zugriffszeit bzw. -dauer und Kosten pro Speicherkapazität in Einklang gebracht werden.

Das rasant wachsende Datenvolumen durch zunehmende ITK-Nutzung, wie z. B. durch E-Mails, erfordert immer mehr Speicherplatz. Um die hierbei entstehenden Kosten zu optimieren (Wirtschaftlichkeitsprinzip), sind Archivierungsstrategien für jene Daten erforderlich, die sich nicht mehr im direkten Zugriff befinden, aber aus Gründen der Nachvollziehbarkeit und Revisionsfähigkeit über einen bestimmten Zeitraum hinweg aufbewahrt und gelesen werden können müssen. Hierbei wird festgelegt, welche Daten ab wann auf welchem Medium für wie lange (z. B. aufgrund gesetzlicher Vorgaben) archiviert werden. Dabei spielt die Lebensdauer der Speichermedien und der Technologie eine wesentliche Rolle.

Archivierung

9.5.23.1.2 Speichermedien

Allgemein können – neben Papier – folgende Klassen von Speichermedien unterschieden werden:

Speichermedien

- Mikrofilm
- Optische Speichermedien
- Magnetische Speichermedien
- Flash-EEPROM
- RAM.

Mikrofilme und Mikroverfilmung kommen oftmals in Archiven, z. B. in Bibliotheken, und bei Banken zum Einsatz. Ihre elektronische Weiterverarbeitung, z. B. in Form einer Schlagwortsuche, ist jedoch schwierig.

Mikrofilme

Optische Speichermedien speichern digitale Signale in Form mikroskopisch feiner Vertiefungen (Pits), die beim Lesen von einem Laserstrahl abgetastet werden. Sie besitzen eine hohe Speicherdichte und kürzere Zugriffszeiten als Magnetbänder. Beispiele für optische Speichermedien sind CD-ROMs, WORMs und DVDs.

*Optische
Speichermedien*

Magnetische Speichermedien nutzen die Polarisierung magnetischer Teilchen, um analoge oder digitale Informationen zu speichern. Zu den magnetischen Speichermedien gehören Disketten, Festplatten und Bänder.

*Magnetische
Speichermedien*

Flash-EEPROMs sind schnelle elektrisch lösch- und programmierbare Festwertspeicher bzw. Nur-Lese-Speicher (Electrically Erasable Programmable Read Only Memory). Sie sind insbesondere beim Schreiben langsamer als RAMs. Sie gehören zu den nichtflüchtigen Spei-

*Flash-
EEPROM*

chern (non-volatile memory). Flash-EEPROMs gelangen in Form von USB-Memory-Sticks als portable Massenspeicher zum Einsatz. Die erwartbare Anzahl der Löschi- und Schreibzyklen ist ebenso wie die Dauer der Speicherung herstellerabhängig recht hoch, aber begrenzt.

RAMs

Ein Random Access Memory (RAM) ist ein Halbleiterspeicher, dessen gespeicherte Informationen bei Abschalten der Betriebsspannung verloren gehen. Er besitzt kurze Zugriffszeiten und wird daher als CPU-naher Speicher bis hin zum Cache verwendet.

*Einsatzgebiete
der Speicher-
medien*

Als Medium zur elektronischen Speicherung in Echtzeit kommen Caches, RAMs sowie Fest- und Wechsellplatten zum Einsatz. Es folgen Speichermedien mit zeitnahe Zugriff wie z. B. WORMs, DVDs bis hin zu Medien mit zeitverzögertem Zugriff, wie Bänder und Bandroboter (Tape Libraries).

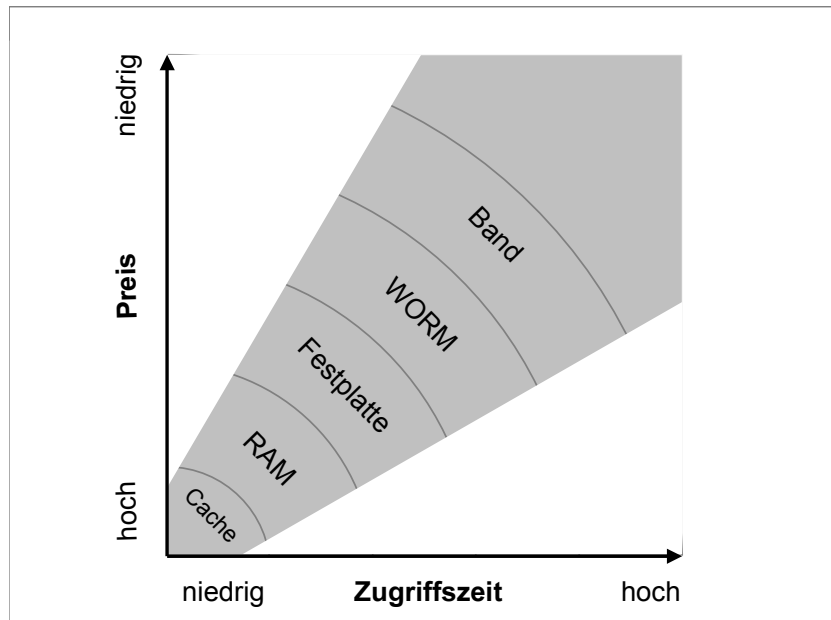


Abb. 9.16: Speichermedien

Bei der Entscheidung, welches Medium in welcher Speicherhierarchie genutzt wird, spielen insbesondere die erforderliche Zugriffszeit bzw. -dauer und die Kosten pro Speicherkapazität eine wesentliche Rolle. Kosten und Zugriffszeit korrelieren meist gegenläufig miteinander. Die Graphik stellt diese Zusammenhänge vom Prinzip her dar.

Ein ebenfalls wichtiges Element bei der Entscheidung für ein Speichermedium ist bei Sekundär- und Tertiärspeichern ihre geforderte Nutzungsdauer. Dieser steht die Lebenserwartung des jeweiligen Speichermediums und der Technologie gegenüber.

*Lebensdauer
von
Sicherungs-
medien*

Risiko veralteter Speichertechnologien

Der technologische Fortschritt führt oftmals zu kostengünstigeren und qualitativ hochwertigeren Lösungen. Hiermit geht häufig einher, dass frühere Technologien zunehmend weniger unterstützt werden, wie z. B. die 5¼-Zoll-Disketten, bis sie schließlich gar nicht mehr angeboten werden. In diesen Fällen begrenzt die Technologie die Nutzungsdauer des Speichermediums.



Präventive Wartung

Die Verantwortlichen sollten Speichermedien und -technologien im Sinne einer präventiven Wartung rechtzeitig vor Ablauf der erwarteten Lebensdauer durch neue Speichermedien bzw. -technologien ersetzen. Dies erfordert eine Beobachtung der technologischen Entwicklungen und Erfahrungen.



Die „Guidelines on best practices for using electronic information“ der Europäischen Gemeinschaft [53] geben folgende Orientierungen zur Lebensdauer verschiedener Speichermedien an:

Medium	Erneuerung
3½-Zoll-Disketten	Sehr kurzfristig
Magnetbänder	Bänder sollten jährlich umgespult und alle 10 bis 15 Jahre ersetzt werden.
CD-ROMs	CD-ROMs sollten alle 10 oder 20 Jahre ersetzt werden.
WORM	WORMs sollten alle 10 oder 20 Jahre ersetzt werden.

Die Studie [54] zeigt, dass die Qualität des jeweiligen Speichermediums sowie die Umgebungsbedingungen, unter denen es aufbewahrt wird, für dessen Lebensdauer wesentlich sind. Tendenziell sinkt die Lebensdauer mit zunehmender Temperatur und Luftfeuchtigkeit, ganz zu schweigen von Rauch und Staub. Instabile Umgebungsbedingungen, wie z. B. Temperatur- und Luftfeuchtigkeitsschwankungen, beeinflussen die Lebensdauer ebenfalls negativ. Bei 20°C und einer relativen Luftfeuchtigkeit von 40 % können gemäß [54] beispielsweise 3480-Magnetbänder und DLTs der betrachteten Hersteller für einen Speicherzeitraum von 5 Jahren akzeptiert werden. Das-

*Produktqualität
und
Umgebungs-
bedingungen*

selbe gilt für die CD-ROMs und WORMs der dort untersuchten Fabrikate. Bei 10°C und 25 % relativer Luftfeuchtigkeit stieg dort die Lebenserwartung dieser Medien auf 20 Jahre.

Primärspeicher

Die Medien für die Primärspeicher sind aufgrund der erforderlichen sehr kurzen Zugriffszeiten vorgegeben: gestuft nach Zugriffszeiten reichen sie vom Cache über RAMs bis zu Festplatten.

Während Cache und RAM im Zuge der Datenverarbeitung temporär genutzt werden, speichern Festplatten den aktuellen Datenbestand des Unternehmens dauerhafter. Ihrem Schutz im Tagesbetrieb gilt daher besondere Aufmerksamkeit.

Disk Arrays

Als Lösung bietet sich der Einsatz redundanter Plattensysteme an. Mehrere physikalische Festplatten werden hierbei logisch so verbunden, dass Datenredundanz entsteht. Patterson, Gibson und Katz an der Universität von Kalifornien in Berkeley arbeiteten Ende der Achtzigerjahre an diesem Konzept und bezeichneten es als Redundant Array of Independent Disks oder kurz RAID. Das RAID Advisory Board ersetzte später „Independent“ durch „Inexpensive“.

RAID-Level, technisch

Der Umfang der Datenredundanz wurde vom RAID Advisory Board (RAB) 1993 in verschiedene Level, RAID 0 bis RAID 5 [55] unterteilt, wobei RAID 0 keine Datenredundanz besitzt. Zu diesen Leveln kamen noch die Level 6 und der nächsthöhere proprietäre Level eines Unternehmens hinzu sowie die Enhanced-Level 1E, 5E und 5EE.

Die Storage Networking Industry Association (SNIA) hat im Juli 2004 die Revision 01.00.00 der Common RAID Disk Data Format (DDF) Specification [56] freigegeben. Sie beschreibt, wie die Daten über die Festplatten einer RAID-Gruppe formatiert werden. Die DDF-Struktur soll eine Basis-Interoperabilität zwischen RAID-Systemen unterschiedlicher Hersteller ermöglichen.

Jeder RAID-Level [56] beschreibt, auf welche Art die Redundanz hergestellt wird. Da moderne Plattensysteme nicht mehr mit Einzel-Bytes, sondern blockweise beschrieben werden und über ein eigenes Verfahren zur Fehlerkorrektur (Error-Correction-Code) verfügen, sind RAID 2 und 3 heute nicht mehr relevant.

Zusätzlich zu den genannten RAID-Leveln gibt es Mischformen, wie z. B. RAID 10 oder RAID 50 als Kombination aus RAID 1 bzw. RAID 5 und RAID 0, welche die Vorteile der Ausfallsicherheit bzw. der Zugriffszeit der jeweiligen Basis-Level in sich vereinigen. Ihre praktische Bedeutung gegenüber den häufiger anzutreffenden RAID-Leveln 1 und 5 ist eher gering.

Bei RAID 0 werden die Daten eines Blocks auf zwei oder mehrere Platten verteilt (Data Striping). Dies führt zu höherer Performance (Datendurchsatz), verringert aber gleichzeitig die Verfügbarkeit, da bei Ausfall nur eines Plattenspeichers alle Daten verloren sind.

*RAID 0:
Speicher-
Parallelisierung*

RAID-Level 1 erfordert 2 Festplatten und ist als Plattenspiegelung (Mirroring) bekannt. Dieser Level bietet 100 %ige Redundanz, wobei die Performance maximal die der Einzeldrives erreicht. RAID Level 1E kombiniert Spiegelung mit Datenverteilung (Data Striping), erfordert minimal 3 Platten und lässt auch eine ungerade Anzahl an Platten zu.

*RAID 1, 1E:
Platten-
spiegelung*

Bei RAID 5 werden Datenblöcke geschrieben. Die Prüfsummen (Parity-Informationen) sind – wie auch die Nutzdaten – über die Platten verteilt. Bei RAID Level 5E wird am Ende jeder Platte ein zusammenhängender Bereich (hot space) für den Fehlerfall freigehalten. Bei Ausfall einer Platte wird dieser Bereich automatisch zugewiesen und dazu genutzt, die „verlorenen“ Daten so wiederherzustellen, dass eine RAID-Level-5-Konfiguration entsteht. Dies ermöglicht einen automatischen Ersatz der fehlerhaften Platte. Bei RAID 5EE sind die hot spaces nicht alle zusammenhängend am Plattenende angelegt, sondern über die Festplatten verteilt. Dies dient dazu, den Durchsatz zu erhöhen und die Zeit für die Fehlerbehebung zu reduzieren [56].

*RAID 5, 5E,
5EE:
verteilte
Prüfsummen*

RAID 6 ist prinzipiell eine Erweiterung des Levels 5 um ein zweites Parity-Schema. Dies erhöht die Fehlertoleranz, so dass der Ausfall zweier Festplatten verkraftet werden kann [56].

*RAID 6: zwei
verteilte
Prüfsummen-
Schemata*

Zusätzlich zur Datenredundanz kann je nach Verfügbarkeitsanforderung die Redundanz weiterer Komponenten erforderlich sein, z. B. Netzteil, Lüfter und SCSI-Controller. Weitere Anforderungen können darin bestehen, Komponenten, z. B. Disks, im laufenden Betrieb zu wechseln (hot swap) oder Platten zusätzlich leer mitlaufen zu lassen (hot spare), um im Fall eines Defekts die Funktion der ausgefallenen Platte übernehmen zu können. Beim Einsatz von hot-spare-Platten können auf dieser bei Ausfall einer redundanten Platte die verlorenen Daten restauriert werden. Während dieser Übergangsphase befindet sich das Platten-Array im kritischen bzw. eingeschränkten Modus, der zu sowohl Performance- als auch Redundanzeinbußen führt.

*Weitere
Redundanz-
anforderungen*

Die Einteilung nach RAID konzentrierte sich auf das zugrunde liegende technische Prinzip. Dies ist für die Anwender eher verwirrend. Daher wurde es vom RAID Advisory Board durch neue Klassifizierungen abgelöst, die sich an der Sicht des Anwenders auf die Verfügbarkeit und den Schutz des Speichersystems orientieren. Es be-

*RAID-Kriterien,
anwender-
orientiert*

schreibt dessen „Extended Data Availability and Protection (EDAP)“-Fähigkeiten.

Das neue System [57] umfasst drei Klassifizierungsstufen (EDAP-Kriterien), die sich an den Verfügbarkeitseigenschaften orientieren. Sie reichen von

- fehlerresistent (FR), der niedrigsten Stufe, über
- fehlertolerant (FT) bis hin zu
- katastrophentolerant (DT).

und bauen hierarchisch aufeinander auf. Die Stufen werden jeweils um eine Kennzeichnung für das Objekt ergänzt, das diese Eigenschaften besitzt. Dies können Plattensysteme (Disk System, DS) oder Array Controller (AC) sein. Innerhalb der Klassifizierungsstufen gibt es neben der Basisstufe bis zu zwei weitere Stufungen, die mit „+“ bzw. „++“ gekennzeichnet sind. Während die Zonen eines katastrophentoleranten Plattensystems (DTDS) beispielsweise 1km auseinander liegen, beträgt diese Distanz bei DTDS + 10km.

9.5.23.1.3 Speichertopologie

*Speicher-
topologie*

Die Speichertopologie ist eine weitere Kategorie beim Speicher-
management. Hier wird (s. a. [58], [59], [60]) unterschieden in

- Direct Attached Storage (DAS)
- Network Attached Storage (NAS) und
- Storage Attached Network (SAN).



Jährliche Verdopplung des Datenvolumens

Einer Marktanalyse von IDC zufolge steigt der Bedarf an Speicherplatz im Zeitraum von 2006–2011 jährlich im Durchschnitt um mehr als 50 % [59].

*DAS, NAS,
SAN*

Bei Direct Attached Storage (DAS), der derzeit verbreitetsten Speicheranbindung, ist das Speichermedium direkt an den Server angeschlossen. Den vielfältigen Anforderungen und dem dynamischen Datenzuwachs ist diese Lösung oftmals nicht mehr gewachsen. Deshalb haben sich NAS- (Network Attached Storage) und SAN-Lösungen (Storage Area Network) am Markt etabliert. Im Gegensatz zu DAS ist das Speichermedium hier nicht direkt am Server angeschlossen, sondern wird über das Netz bereit gestellt. NAS befindet sich zwischen Anwendungsserver und dem Dateisystem und stellt Dateien bereit. Er arbeitet somit als dedizierter Daten- bzw. Fileserver. Demgegenüber stellen SANs das Speichermedium selbst bereit, z. B. in Form von Festplatten oder Bandbibliotheken.

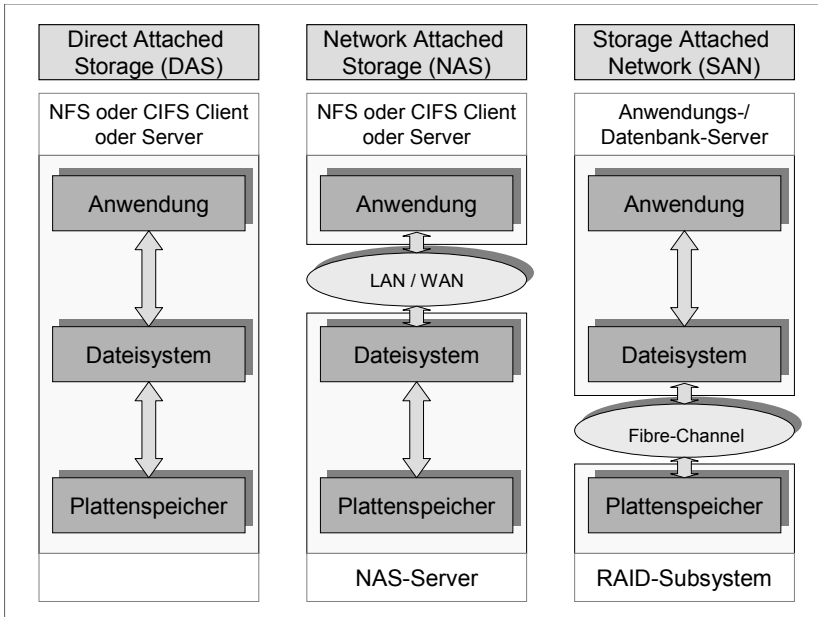


Abb. 9.17: DAS, NAS, SAN

Bei DAS verbinden unterschiedliche Adapter das Speichermedium direkt mit dem Computer. Die Adapter nutzen standardisierte Software-Protokolle, wie SCSI, Fibre-Channel etc. Diese Standards sind jedoch so flexibel, dass es für die verschiedenen UNIX®- und Windows®-Systeme eine Vielzahl unterschiedlicher SCSI- und Fibre-Channel-Varianten gibt [58].

NAS-Systeme können als fertige Lösung angeschafft und in ein bestehendes LAN integriert werden [58]. Die am LAN angeschlossenen Clients erkennen die NAS-Systeme als Fileserver und nutzen sie. NAS-Systeme sind netzzentriert (network centric). Sie lassen sich über verschiedene Netzprotokolle, z. B. TCP/IP für die Datenübertragung und Ethernet oder Gigabit-Ethernet als Übertragungsmedium, ansprechen. Sie stellen unterschiedliche Dateisysteme zur Verfügung, z. B. CIFS (Common Internet File System) für Microsoft®-Windows®-Umgebungen, NFS (Network File System) für UNIX®-Umgebungen sowie FTP, http und andere Netzprotokolle. NAS-Systeme ermöglichen heterogenen Clients den Zugriff auf einen zentralen Datenbestand. Die bessere Speicherauslastung, das zentrale Management und die leichte Installierbarkeit machen NAS-Systeme zu einer kos-

DAS

*Network
Attached
Storage (NAS):
Fileserver im
LAN*

tengünstigen Lösung zur Erweiterung der Speicherkapazität. Durch den Datentransfer belasten sie aber das LAN.

Storage Area Network (SAN):
Speichermedien im separaten Hochgeschwindigkeitsnetz

Speichernetze, englisch Storage Area Networks oder kurz SANs, stellen separate Hochgeschwindigkeitsnetzwerke dar, z. B. in Form eines Fibre-Channel-Netzes (FC-SAN). Sie sind für den Anschluss unterschiedlicher Speichermedien an Server konzipiert. Hierbei kann unterschieden werden in SANs, welche die Fibre-Channel-Arbitrated-Loop (FC-AL) nutzen und den Fabrics (Gewebe). Bei FC-AL (Ringtopologie) verbindet ein Hub bis zu 127 Geräte, bei Fabrics verknüpfen Switches eine Vielzahl von Servern und Speichereinheiten [60]. SAN-typische Sicherungsfunktionen sind Momentaufnahmen (snapshot copies), synchrone Spiegelung (Mirroring) und asynchrone Spiegelung.

Vorteile der SAN-Architektur liegen u. a. in der modularen Struktur, in der besseren Ausnutzungsmöglichkeit der Speicherressourcen, dem zentralen Management und der Entlastung des LANs durch den Aufbau einer eigenen Netzinfrastruktur. Die modulare Struktur erlaubt eine einfachere Skalierbarkeit bei gleichzeitigem Datenzugriff. Durch die eigene Netzinfrastruktur des SANs lassen sich Datensicherungen und –archivierungen LAN-unabhängig ausführen.

Speicher-virtualisierung

SANs bieten einen weiteren Vorteil: die Virtualisierung des Speicherplatzes durch „virtuelle“ Plattenspeicher. Dieses Prinzip ist aus der Großrechnerwelt bekannt, in der mit virtuellem Hauptspeicher gearbeitet wird. Die Virtualisierung des Speichers transformiert die physikalischen in logische Speichervolumina, die LUNs (Logical Unit Number). Für die Server bzw. Hostsysteme sind nur die logischen Speichervolumina „sichtbar“. So können beliebige Speicherkomponenten, z. B. RAIDs (Redundant Array of Inexpensive Disks), preiswertere JBODs (Just a Bunch of Disks), oder auch MBODs (Managed Bunch of Disks) sowie SBODs (Switched Bunch of Disks) unterschiedlicher Hersteller im SAN genutzt werden. Kapazitäten lassen sich dadurch prinzipiell zentral und dynamisch zuweisen und verändern sowie die Gesamtnutzung des Speicherpools (Storage-Pool) optimieren.

JBOD

Worin unterscheiden sich JBODs, MBODs und SBODs [61]? Bei JBODs sind die Platten vom Platten-Controller ausgehend in einer Kette hintereinandergeschaltet. Deren Ende führt wieder zum redundant ausgelegten Controller, so dass sich eine logische Schleife ergibt. Fällt eine Platte oder eine Verbindung aus, so hat der Controller keinen Zugriff mehr und das JBOD-System fällt aus.

MBODs verwenden demgegenüber einen zentralen Hub. Dadurch lassen sich einzelne Platten aus der Schleife herausnehmen, ohne dass die Datenübertragung zum Erliegen kommt. Der zentrale Hub ermöglicht zusätzlich die Sammlung statistischer Daten, die Ermittlung der Fehlerhäufigkeit und der Auslastung. Sowohl JBODs als auch MBODs haben prinzipbedingte Nachteile, weil stets nur einer der beiden redundanten Controller aktiv sein kann. Außerdem müssen die Datenpakete die logische Schleife durchlaufen, bis sie zur Zielpalte gelangen. Hierdurch ergeben sich Latenzzeiten.

MBOD

Diese Nachteile vermeiden SBODs. Ähnlich wie bei Switches ist die Steuereinheit eines SBODs in der Lage, mehrere Verbindungen offen zu halten. Dadurch können beide Controller Daten an unterschiedliche Platteneinheiten übertragen, ohne sich gegenseitig zu behindern. Die Latenzzeit, die sich aus dem Durchlaufen der logischen Schleife ergibt, vermeiden SBODs ebenfalls. Soll der SBOD-Switch eine Verbindung zwischen dem Controller und einer Platteneinheit aufbauen, bildet er zwischen diesen eine direkte virtuelle Schleife.

SBOD

Bei der Virtualisierung unterscheidet die SNIA (Storage Networking Industry Association) zwischen In-Band-Virtualisierung und Out-of-Band-Virtualisierung. Bei der In-Band-Virtualisierung befindet sich die Steuerungsinstanz für den Datenstrom, die so genannte Appliance im Datenpfad zwischen Server und Speicher. Hier laufen sowohl die Steuerungs- als auch die Nutzdaten über die Appliance, in der die Zuordnung der Speichersegmente (LUN) zu den einzelnen Servern erfolgt. Bei der Out-of-Band-Virtualisierung befindet sie sich außerhalb des Datenpfades und kommuniziert über das LAN mit dem Host-Based-Adapter (HBA) des jeweiligen Servers. In der Appliance sind die logischen Speichersegmente je Server definiert. Im HBA sind die exakten Informationen über die zugehörigen logischen und physikalischen Blöcke gespeichert.

*In-Band- und
Out-of-Band-
Virtualisierung*

Unter Kosten-Nutzen-Aspekten sind auch die Interoperabilität und das Management heterogener SANs für Unternehmen ein wichtiges Element bei der Entscheidung für oder gegen eine SAN-Lösung. Um dem gerecht zu werden, hat die SNIA die Storage Management Initiative Specification (SMI-S) publiziert [62]. Sie beschreibt die Schnittstelle, die dem sicheren und interoperablen Management heterogener verteilter Speichersysteme in einem SAN dient.

Die Schnittstelle nutzt ein objektorientiertes und XML-basierendes Protokoll zwischen Server und Client. Als Basistechnologie kommt Web Based Enterprise Management (WBEM) zum Einsatz. Dieser Satz an Technologien zum interoperablen Management eines Unternehmens besteht aus CIM, XML und http.

Das Common Information Model (CIM) beschreibt Informationen zum Management der zu verwaltenden Objekte, wie Systeme, Netze, Anwendungen und Services. CIM ist ein Standard der Distributed Management Task Force (DMTF®), der in der Version 2.15 im April 2007 veröffentlicht wurde. Die Tags zur Darstellung der entsprechenden Daten im Protokoll sind in XML definiert.

*Redundante
Speicher-
topologie*

Zur Absicherung der jeweiligen Speicherlösung sind die Anforderungen an die Betriebssicherheit zu berücksichtigen. Unter Anwendung des Redundanzprinzips führt dies bis hin zur Redundanz und hinreichenden räumlichen Trennung aller aktiven und passiven Komponenten des Speichernetzes, der Speichermedien und des Speicher-managements.

*iSCSI, iFCP
und FCIP*

Da die Anforderungen an die Distanz räumlich bzw. geographisch verteilter Speichereinheiten zunimmt, gewinnen Protokolle zur Übertragung über IP an Bedeutung. Hierzu gehören das Internet SCSI (iSCSI) [63], das Internet Fibre Channel Protocol (iFCP) und Fibre Channel over IP (FCIP) [64]. FCIP ist ein Protokoll, das geographisch verteilte FC-SANs transparent über IP-Netze verbindet.

*Virtuelle
Bandbibliothek*

Virtuelle Bandbibliotheken (s. a. [65]) (Virtual Tape Library, VTL) bestehen aus Disk-Arrays, die per Software die Funktionen von Bandbibliotheken emulieren. Die im Vergleich zu den Bandbibliotheken schnellen Disk-Arrays beschleunigen den Backup- und Restore-Vorgang.

VTLs nutzen verschiedentlich De-Duplizierung zur Einsparung von Speicherplatz. De-Duplizierung kann das Speichervolumen je nach Art der Daten auf ein Zehntel bis hin zu einem Fünfzigstel reduzieren [65]. Die De-Duplizierung erfolgt entweder durch eine In-Line-Appliance bereits während der Datensicherung oder nach Abschluss des Backups. Die In-Line-Appliance reduziert die Backup-Geschwindigkeit. Um dies zu optimieren, speichert sie die Daten zuerst und analysiert sie um einige Sekunden zeitversetzt.

9.5.23.2 Firewall

Firewall

Ein Firewall (s. a. [37], [66], [67], [68]) ist eine Netzkomponente, die zwei Netze mit unterschiedlichem Sicherheitsniveau miteinander so verbindet, dass das zu sichernde Netz vor Übergriffen aus dem anderen Netz geschützt wird. Entsprechend dem OSI-7-Schichten-Modell der ISO arbeiten Firewalls auf den Schichten (layers) 2, 3, 4 und 7.

Die Schichten 1–4 des OSI-7-Schichten-Modells [69] sind die transportorientierten Schichten, die Schichten 5–7 die anwendungsorientierten Schichten. Die wichtigste Aufgabe der Schicht 3, Vermitt-

lungsschicht (network layer), ist die Ermittlung eines optimalen Weges durch ein verzweigtes Netz (Routing). Sie stellt eine Ende-zu-Ende-Verbindung zwischen zwei kommunizierenden Stationen her und sorgt dafür, dass ein Paket – egal auf welchem Weg – bei der richtigen Station (Adresse) ankommt.

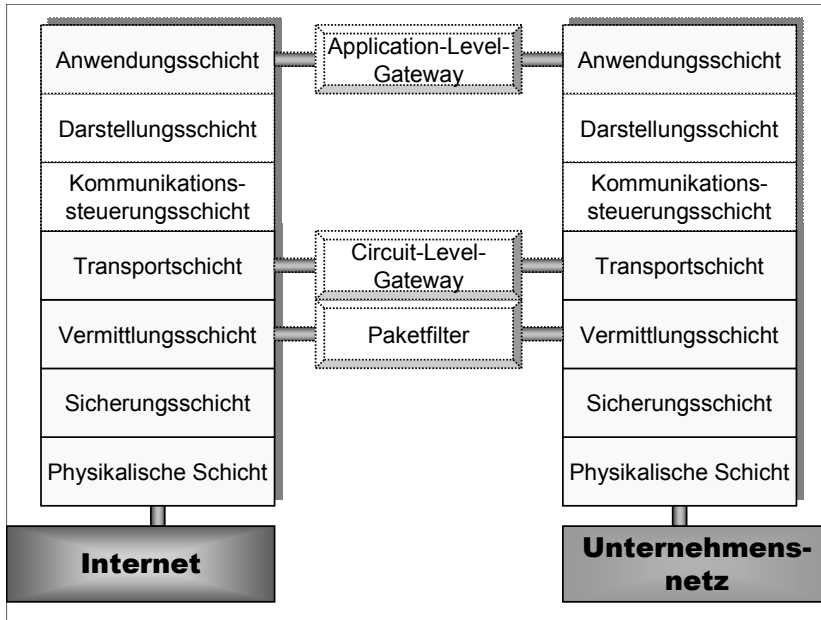


Abb. 9.18: Firewall-Ebenen (Prinzipdarstellung)

Im Internet werden Schicht-3-Adressen durch IP-(Internet-Protocol-) Adressen repräsentiert. Die Protokolle der Transportschicht (transport layer) realisieren eine Ende-zu-Ende-Verbindung zwischen einzelnen Prozessen verschiedener Endsysteme. Die in der TCP/IP-Terminologie vorkommenden Ports können als Endpunkte (Quell- und Ziel-Port) solcher Prozesse verstanden werden.

Entsprechend der Ebene des OSI-7-Schichten-Modells, auf welcher der Firewall filtert, gibt es drei Firewall-Arten:

- Paketfilter
- Circuit-Level-Gateway
- Application-Level-Gateway.

<i>Paketfilter</i>	Ein Paketfilter (s. a. [70], [37], [66], [67], [71]) führt die Filterung primär auf der OSI-Schicht 3 der jeweiligen Kommunikationsprotokolle durch. Paketfilter können dementsprechend filtern nach: • Quell- und Zieladresse (OSI-Schicht 3; IP: Quell- und Zieladresse) • Protokoll-Typ (Ethernet: OSI-Schicht 2; IP: OSI-Schicht 3) • Quell- und Ziel-Ports (OSI-Schicht 4) • benutzerdefinierten Bitmasken.
<i>Paketfilter mit Zustandstabelle</i>	Je größer und komplexer die Netze werden, desto unübersichtlicher werden die dazugehörigen Filtertabellen. Hinzu kommt, dass Paketfilter über kein „Gedächtnis“ verfügen, sodass sie Zusammenhänge zwischen aufeinander folgenden Paketen nicht bewerten können. Hierdurch sind sie leicht zu überlisten. Dies führt dazu, dass Paketfilter entweder nur als Vorfilter zum Einsatz kommen oder mit einer Zustandstabelle [71] versehen werden. Was wird hierdurch erreicht? Ein Paketfilter müsste gemäß TCP-Spezifikation z. B. eingehende Pakete an alle Portnummern größer als 1023 und kleiner als 16384 zulassen. Dadurch entsteht jedoch ein hohes Risiko, dass unautorisierte Nutzer über diese Ports durch verschiedenartige Techniken in das zu schützende Netz eindringen. Paketfilter mit Zustandstabelle lösen u. a. dieses Problem, indem sie sich ein Verzeichnis der ausgehenden TCP-Verbindungen sowie der dazugehörigen Client-Ports erstellen. Mittels dieser „Zustandstabelle“ überprüfen sie eingehende Pakete. Im Ergebnis bedeutet dies, dass Paketfilter mit Zustandstabelle die Standard-Funktionalität eines Paketfilters um Prüfungen in der OSI-Schicht 4 erweitern.
<i>Circuit-Level-Gateway</i>	Ein Circuit-Level-Gateway (s. a. [37], [67]) führt die Filterung auf Verbindungsebene durch. Das Circuit-Level-Gateway arbeitet sozusagen als Vermittlungsstelle für das betreffende Protokoll.
<i>Application Level Gateway</i>	Das Application Level Gateway (s. a. [37], [66], [67], [70], [71]) ist ein Firewall, der sich aus Sicht eines Client-Programms wie ein Anwendungs-Server für den betreffenden Dienst, z. B. DNS, http, https, ftp, LDAP, SMTP, Telnet, darstellt. Diese Anwendungs-Server im Firewall übernehmen stellvertretend, d. h. als Proxy (Stellvertreter), die Aufgaben des jeweiligen Dienstes. Dadurch kommt keine direkte Verbindung zum internen Netz zustande. Die Proxies verbergen damit das interne Netz gegenüber dem äußeren. Application Level Gateways (ALG) bieten üblicherweise umfangreiche Protokollierungs-(Logging-)Funktionalitäten, da sie das komplette übertragene Paket prüfen können. So lassen sich anwendungsspezifische Kommandos innerhalb des Pakets protokollieren. Dem Vor-

teil der „Komplett-Paket-Prüfbarkeit“ steht der potenzielle Nachteil eines geringeren Durchsatzes gegenüber, da das Lesen und Prüfen der kompletten Pakete Zeit benötigt. Deshalb eignen sich Application Level Gateways prinzipiell weniger für breitbandige Echtzeitanwendungen. Daher realisieren Unternehmen bei entsprechenden Sicherheits- und Performanceanforderungen einen mehrstufigen Schutz, indem sie die Anbindung an das Internet über ein im Vergleich zum ALG schnelleren Paketfilter realisieren, gefolgt von einem Application Level Gateway und einem erneuten Paketfilter.

Web Application Firewalls (WAF) bzw. WebShields befinden sich als Proxy, also als Stellvertreter der jeweiligen Webanwendung, zwischen Browser und Webanwendung und filtern den Datenstrom. Durch die Filterung ergeben sich Performance-Einbußen. Ein WAF dient als zusätzliche Sicherheitsmaßnahme im Sinne eines Vorfilters, der eine Validierung des Inputs durchführt. Dies kann z. B. das Filtern unzulässiger Zeichen betreffen oder die Verhinderung von Anomalien. Die Berücksichtigung sicherheitsrelevanter Aspekte sowie das Abfangen potenzieller Angriffe obliegt jedoch weiterhin vorrangig auch der Webapplikation. Web Shields können regelbasiert beispielsweise XSS und SQL-Injection erkennen und auf vorgegebene Weise darauf reagieren. Für den modular aufgebauten open source Apache-Webserver existiert als open source WAF das Modul ModSecurity bzw. mod_security.

*Web
Application
Firewall*

Ein entscheidender Faktor bei der Erreichung des gewünschten Schutzes durch Firewalls sind die Filterregeln. Diese aufzustellen und einzurichten erfordert Erfahrung und Sorgfalt. Beispielsweise sind für Paketfilter die erlaubten Verbindungen anzugeben, für ALGs die erlaubten Dienste. Die Vorgaben sind zu dokumentieren und die eingerichteten Filterregeln zu protokollieren und zu testen.

Neben der Unterscheidung nach der Ebene des OSI-7-Schichten-Modells, auf welcher der Firewall filtert, kann unterschieden werden in

*Router,
Appliance und
Host als
Firewall*

- Firewalls in Routern (Begrenzungsrouter)
- Firewall Appliances
- Firewalls in Computer-Systemen (Bastion-Host).

Der Einsatz von Routern als Firewall (Begrenzungsrouter) setzt in den Routern die – meist vorhandene – Paketfilter-Funktionalität voraus. Allerdings sind die Möglichkeiten derartiger Firewalls begrenzt.

*Begrenzungs-
router*

Firewall Appliances sind spezifisch für die Aufgabe als Firewall ausgelegte, autonome und in der Regel proprietäre Komponenten, be-

Appliance

stehend aus Hard- und Software. Sie sind quasi „schlüssel-fertig“ vorkonfiguriert. Ihre Inbetriebnahme benötigt wenig Zeit und die Konfiguration ist relativ einfach gestaltet. Sie sollten über automatische Update-Funktionen verfügen. Die Erweiterungsmöglichkeiten der Appliances sind oftmals begrenzt.

Bastion-Host Firewalls in Computern, die sich zwischen dem zu sichernden und dem ungesicherten Netz befinden, heißen Bastion-Host (Bollwerk). Sie können als Paketfilter, Circuit-Level- oder Application Level Gateway konfiguriert sein. Besitzt ein Bastion-Host mehrere Netzwerk-Karten, so wird er als „Multi-Home“-Firewall, bei zwei Netzwerk-Karten als „Dual-Home“-Firewall bezeichnet.

Bastion-Hosts können in unterschiedlichen Topologien eingesetzt werden. Dementsprechend kann unterschieden werden in

- Bastion-Host mit entmilitarisierter Zone
- kaskadierter Bastion-Host
- Bastion-Host mit Secure-Server-Netz.

Bastion-Host mit entmilitarisierter Zone Bei Einsatz von zwei Firewalls, z. B. einem Begrenzungsrouter und einem Bastion-Host, entsteht zwischen diesen eine entmilitarisierte Zone. In dieser können z. B. Web- oder FTP-Server angesiedelt werden. Durch den Begrenzungsrouter sind die Server zwar geschützt, befinden sich jedoch noch vor dem Firewall, von dem sie als „nicht vertrauenswürdig“ eingestuft werden. Sie sind somit einem höheren Risiko ausgesetzt als das hinter dem Bastion-Host liegende Netz. Daher werden sie auch als „Opferlamm“ (Sacrificial Host) bezeichnet.

Kaskadierte Bastion-Hosts Größeren Schutz bieten kaskadierte Bastion-Hosts. Hierbei werden mehrere Firewalls hintereinander geschaltet, sodass – wie beim Sicherheitsschalenmodell, allerdings innerhalb der „Zugangsschale“ – mehrere zusätzliche Schalen bzw. Sicherheitszonen entstehen, die ein potenzieller Angreifer überwinden muss. Eine mögliche Konfiguration ist eine Hintereinanderschaltung zweier Bastion-Hosts mit entmilitarisierter Zone.

Bastion-Host mit Secure-Server-Network Eine Variante der kaskadierten Bastion-Hosts ist der Bastion-Host mit Secure-Server-Network. Anstelle mehrerer kaskadierter Bastion-Hosts wird ein Bastion-Host mit mindestens drei Netzwerk-Karten ausgestattet. Wie beim „Dual-Home“-Firewall stellt eine Netzwerk-Karte die Verbindung ins Internet und eine zum LAN her, während weitere Netzwerk-Karten Verbindungen z. B. zu Web-Servern oder RAS-Servern herstellen.

Organisationen und Unternehmen sind in ihrem Betriebsablauf zunehmend auf das Internet angewiesen, beispielsweise hinsichtlich der E-Mail-Korrespondenz, Recherchen, Onlinebanking, Onlineshopping etc. Eine Störung dieser Verbindung kann damit massiven Einfluss auf die Handlungsfähigkeit des Unternehmens haben. Daher ist sicherzustellen, dass der Firewall ebenso wie die Netzanbindung anforderungsgemäß ausreichend redundant ausgelegt sind und keinen „Single Point of Failure“ darstellen.

9.5.23.3 Intrusion-Detection-, -Response-, -Prevention-System

Intrusion-Detection-Systeme (s. a. [67], [70], [72]) dienen dazu, Angriffe frühzeitig zu erkennen. Es lassen sich zwei Arten der Angriffserkennung unterscheiden:

- Anomalieerkennung
- Mustererkennung

Anomalien stellen Abweichungen vom Normalzustand dar. Sie können statistischer Natur sein oder in Abweichungen vom definierten Protokoll liegen. Statistische Anomalien sind beispielsweise Abweichungen von den entlang der Zeitachse als normal festgelegten CPU- oder Netzauslastungsprofilen. Überschreitet die Abweichung bestimmte Grenzwerte, so wird dies als Angriffsversuch angesehen. Eine andere Form der Anomalie könnte ein besonders hoch privilegierter Zugriff auf Daten sein, den dieser Benutzer üblicherweise nicht ausübt. Protokollanomalien sind Abweichungen im Kommunikationsablauf, d. h. es kommt ein Paket, das z. B. im aktuellen Protokollstatus nicht zulässig ist.

Die Mustererkennung basiert auf der Annahme, dass Angriffe an charakteristischen Ereignismustern (Intrusion-Signatures) erkennbar sind. Beispielsweise spricht ein Angreifer beim Portscanning im Vorfeld eines Angriffs die unterschiedlichen TCP-Ports an, um festzustellen, wo ein Dienst installiert ist, den er angreifen kann. Wenngleich dies für einen Angriff charakteristisch ist, so ist die Erkennung insofern schwierig, als Angreifer die Ports in beliebiger Reihenfolge und in zufälligen Zeitabständen sowie von unterschiedlichen Absenderadressen aus ansprechen können.

Intrusion-Detection-Systeme lassen sich nach der Art der Datenaufnahme unterscheiden in netzbasierte und hostbasierte. Netzbasierte IDS (NIDS) befinden sich an einer Stelle im Netz. Dort erfassen sie die Daten über ein Sniffer-Interface, analysieren den Datenstrom nach vordefinierten Regeln und setzen bei einer Angriffs-

*Intrusion-
Detection-
System*

*Anomalie-
erkennung
Muster-
erkennung*

*Netzbasierte
IDS (NIDS)*

erkennung Alarmmeldungen ab, z. B. in Form eines Alarms an der Konsole oder einer E-Mail oder SMS an den Administrator.

*NIDS: Vor-
und Nachteile*

NIDS können installiert werden, ohne sich auf den Rest des Netzwerks auszuwirken. Üblicherweise laufen sie auf separaten Appliances und belasten keine Endsysteme. Das NIDS wird im „promiscuous mode“ (promiscuous = wahllos) betrieben, so dass es „wahllos“ alle Frames, nicht nur die an es adressierten, der OSI-Schicht 2 mithört. Außerdem befindet es sich im „stealth mode“ (Tarnkappenmodus), so dass es im Netz nicht mehr „sichtbar“ ist und nicht angesprochen werden kann. Netzbasierte IDS können keine verschlüsselten Daten analysieren.

*Hostbasierte
IDS (HIDS)*

Hostbasierte IDS (HIDS) sind Teil der Protokollierungsfunktionalität eines Rechners (Host) und werten System-, Prüf- und Ereignisprotokolle (Ereignis-Logs) aus. Da ein HIDS auf dem Rechner selbst läuft, benötigt es Systemressourcen und kann von einem Angreifer leichter erkannt werden. Es stützt sich in der Regel auf die Protokolldateien und zieht daher die aktuelle Netzkommunikation nicht mit ein. Im Gegensatz zu einem NIDS befasst es sich nur mit dem Datenverkehr desjenigen Rechners, auf dem es installiert ist, und benötigt demgegenüber somit weniger Systemressourcen. Außerdem beobachtet es zusätzlich die Reaktion des Rechners. HIDS haben in den letzten Jahren an Bedeutung verloren und werden von NNIDS verdrängt.

*Network Node-
based IDS
(NNIDS)*

Network Node-based IDS (NNIDS) befinden sich direkt auf dem Rechner. Sie befassen sich mit dem laufenden Datenverkehr zu und von diesem Rechner. Zusätzlich zum Datenverkehr analysieren sie Ereignisse auf Betriebssystemebene, z. B. fehlerhafte Anmeldeversuche und unerlaubte Zugriffe auf Systemdateien. Ein NNIDS benötigt Systemressourcen und ist für einen Angreifer erkennbar.

*Alarmierung,
Meldung*

Eine klare Begriffstrennung zwischen Intrusion-Detection-Systemen (IDS), Intrusion-Response-Systemen (IRS) und Intrusion-Prevention- bzw. Protection-Systemen (IPS) ist derzeit nicht erkennbar. Intrusion-Detection-Systeme dienen jedoch primär der Erkennung und Alarmierung.

IRS: Reaktion

Ein Intrusion-Response-System ermöglicht es darüber hinaus, Sicherheitsmaßnahmen zu initiieren, z. B. den Firewall umzukonfigurieren, Verbindungen zu blockieren und Logging-Mechanismen zu aktivieren.

*Intrusion
Prevention
System (IPS)*

Für die Kombination aus Intrusion-Detection und Intrusion-Response findet sich auch der Begriff Intrusion-Prevention bzw. Intrusion-Protection, der allerdings noch weiter zu fassen ist. Derartige Systeme erstrecken sich bis hin zur Erkennung und Behandlung von Proto-

kollanomalien, Phishing, Cross Site Scripting (XSS), DoS, DDoS, SQL injection, Würmer, etc. Sie nutzen hierzu u. a. Mustererkennung, Protokollanalysen und statistische Analysen. Befindet sich ein IPS direkt im Übertragungsweg, so kann es den Datenverkehr aktiv sperren oder Datenpakete verwerfen, wenn es einen Angriff erkennt. Hierbei existiert das Risiko eines Single Point of Failure (SPoF), wenn das IPS ausfällt oder fehlerhaft reagiert.

„Honigtöpfchen“ (Honeypots) sind eine spezielle Form der Einbruchserkennung. Hierzu bauen Verteidiger in einem geschützten Netz Attrappen für potenzielle Angreifer auf und statuen sie mit interessant klingenden Namen und Dateien aus. Bricht ein Angreifer in das Netz ein, wird sein Interesse vom Honigtöpfchen geweckt und er arbeitet sich in diese Richtung vor. Hierbei löst er einen Alarm aus, sodass der Verteidiger dessen Aktivitäten aufzeichnen und für die Verfolgung nutzen kann.

Honigtöpfchen

Honeypots lassen sich in low, medium und high interactive unterscheiden. Low-Interaction-Honeypots zeichnen auf (logging). Medium-Interaction-Honeypots emulieren nur bestimmte Software und deren Schwachstellen. Beispiele hierfür sind honeyd, eine Open Source Software, honeytrap und nepenthes. In der Botanik bezeichnet Nepenthes eine Gattung fleischfressender Pflanzen. High-Interaction-Honeypots repräsentieren meist einen für Angreifer wertvollen Computer, z. B. einen vollständig ausgestatteten Server, der potenziellen Angreifern als Ganzes zur Verfügung steht. Der Verteidiger überwacht den Server, z. B. mit Hilfe von Sebek®, einem Werkzeug, das zur Aufzeichnung der Aktivitäten eines Angreifers auf einem Honeypot entworfen wurde.

Eine Erweiterung des Honigtöpfchens stellt ein „Honignetz“ (Honeynet) dar, wie es von The Honeynet Project® [73] vorgeschlagen wurde. Hier sind verschiedene Systeme (Honigtöpfe) zu einem Netz (Honignetz) zusammengeschaltet. Es dient dazu, die Methoden und Werkzeuge der Angreifer kennenzulernen und zu analysieren, um Vorgehensweisen zu deren Abwehr zu entwickeln. Ein Honignetz erfordert gegenüber einem Honigtöpfchen mehr Aufwand und Administration. Gleichzeitig steigt das Risiko, dass durch Kompromittieren des Honignetzes Gefahren für externe Systeme ausgehen. Im Gegensatz zu herkömmlichen Honigtöpfchen ist es eher als Forschungswerkzeug zu sehen, das Informationen über mögliche Bedrohungen und Angriffsmethoden sammelt.

Honignetz

The Honeynet Project® [73], eine Non-Profit-Forschungseinrichtung, hat ein solches Forschungsnetz aufgebaut. In der Phase 1 von 1999–2001 wurde das GenI-(1. Generation)-Honignetz aufgebaut, über-

Das Honeynet Project®

wacht und die gesammelten Daten ausgewertet. Während der Phase 2 von 2002–2003 wurde ein gereifteres Honignetz (GenII) eingerichtet, das leichter einzusetzen und schwieriger zu entdecken ist sowie Daten effizienter sammelt. Es zielt auf erfahrene Angreifer ab. Außerdem wurden in dieser Phase virtuelle Honignetze entwickelt. Hierbei läuft das gesamte Honignetz und damit auch die verschiedenen echten Betriebssysteme auf einem einzigen System. Dies vereinfacht den Aufbau und die Verwaltung des Honignetzes. Darüber hinaus wurde eine Forschungsallianz ins Leben gerufen, welche die Honignetz-Forschung rund um den Globus koordiniert.

In der dritten Phase von 2003–2004 erstellte The Honeynet Project® eine bootbare CD-ROM, die alle jene Anforderungen zur Datensteuerung und -sammlung enthält, die das Aufsetzen eines Honignetzes leichter machen und die zu sammelnden Daten standardisieren. Inzwischen gibt es weltweit verschiedene Honeynet-Projekte. The Honeynet Project®, Honeypots und Honeynet-Technologien sowie Computer-Forensik sind im Buch „Know Your Enemy“, 2nd edition, beschrieben.

Honeytoken

Honeytokens sind ungenutzte Daten, die ein Verteidiger aufstellt, um Angreifer anzulocken. Beispiele hierfür sind „erfundene“ bzw. nicht vergebene E-Mail- und IP-Adressen oder auch Datenbankeinträge oder Dateien.

Teergrube, Teerfalle

Eine „Teergrube“ bzw. „Teerfalle“ (Tarpit), auch „klebriger Honigtopf“ (Sticky Honeypot) genannt, ist ein Server, der unerwünschte Verbindungen annimmt und künstlich verlangsamt. Zum Einsatz kommen Teerfallen gegen Spam, Würmer und Portscans. Unerwünschte Verbindungsversuche erkennt die Teerfalle daran, dass es sich bei der Zieladresse um eine nicht vergebene IP-Adresse handelt. Teerfallen können im OSI-Schichtenmodell auf IP-, TCP- oder Anwendungsebene arbeiten.

Die Teerfalle beantwortet im ersten Schritt den Verbindungswunsch zur nicht existenten IP-Adresse, verzögert die Antwort jedoch. Sie täuscht anschließend weiterhin vor, die gewünschte IP-Adresse zu sein. In der dann folgenden Kommunikation zögert sie Antwortpakete hinaus. Zusätzlich minimiert sie diese, sendet falsche Antwortpakete oder lässt welche aus und meldet Verbindungsfehler, ganz nach Belieben. Der angreifende Kommunikationspartner wartet dadurch, läuft auf time-outs und allokiert Ressourcen für die Kommunikation.

Ein Beispiel für eine Teerfalle ist LaBrea [74]. LaBrea übernimmt ungenutzte IP-Adressen und baut für diese virtuelle Server. Diese bear-

beiten eventuelle Verbindungsversuche in der Form, dass der unerwünschte Kommunikationspartner möglichst lange „festklebt“.

9.5.23.4 Content-Security-Systeme

Content-Security-Systeme prüfen den Absender und Inhalt ein- und ausgehender E-Mails. Hierzu nutzen sie ein unternehmensspezifisch festgelegtes Regelwerk. So kann das System unerwünschte E-Mails mit Werbebotschaften, die Spam-Mails, prinzipiell von Newslettern unterscheiden, sie kennzeichnen, herausfiltern, in Quarantäne schicken und gegebenenfalls löschen. Die Verringerung der Werbeflut erspart zum einen den potenziellen Empfängern den Zeitaufwand für deren Durchsicht. Zum anderen kann der in Spam-Mails eventuell enthaltene bösartige Code, z. B. in Form von Dialern oder Viren, gleich mit vernichtet werden.

Ein Content-Security-System analysiert eingehende E-Mails im Hinblick auf Absender und Empfänger. Anhand einer „weißen Liste“ (whitelist) erkennt es bekannte und zugelassene Absender und über eine „schwarze Liste“ (blacklist) bekannte und unerwünschte Absender. Die Wirksamkeit der „schwarzen Liste“ ist – wie bei allen negativen Sicherheitsmodellen – eingeschränkt, weil sie die Kenntnis aller unerwünschten Absenderadressen voraussetzt. Dies ist erfahrungsgemäß jedoch nur bedingt möglich, zumal die Spam-Versender ihre Adressen häufig ändern.

*Inhaltsprüfung,
Spam-Filter*

Das Content-Security-System analysiert auch den Betreff und den Text der Nachricht anhand vordefinierter „schwarzer Listen“ mit gewichteten Schlüsselwörtern und charakteristische Textpassagen. Diese Listen enthalten z. B. Schlüsselwörter wie „Sex“ und „Viagra“, die in Spam-Mails häufig vorkommen und charakteristische Textpassagen, wie „Ihr Konto wurde gesperrt“ u.ä.

Zur Rekonstruktion der Originalinhalte zerlegt das Content-Security-System die E-Mail gegebenenfalls in ihre einzelnen Komponenten. Hierzu dekomprimiert es z. B. komprimierte Dateien, d. h. entpackt sie. Die Bestandteile der E-Mail unterzieht das System einer Virenprüfung. Anschließend untersucht es die geprüften Elemente auf die im Regelwerk definierten Stichwörter.

Ausgehende E-Mails können ebenfalls analysiert werden. Hierdurch soll beispielsweise vermieden werden, dass E-Mails mit speziellen Texten, z. B. „vertraulich“ oder „geheim“ an unbekannte Adressaten verschickt werden.

*Ausgehende
E-Mails*

9.5.23.5 Computerviren-Suchprogramme

<i>Viren</i>	Computerviren und Makroviren gehören ebenso wie Computervürmer und trojanische Pferde zur Schadsoftware. Viren benötigen einen Wirt. Programmviren nutzen Programme als Wirt. Sie verbreiten sich, wenn der Benutzer das virulente Programm aufruft. Der Virus sucht dann noch nicht befallene Programme und kopiert sich in diese hinein. Demgegenüber verbreiten sich Makroviren über Dateien, also elektronische Dokumente. Makroviren benutzen Makro- oder Skript-Sprachen, wie sie z. B. in Textverarbeitungsprogrammen enthalten sind. Viren lassen sich ferner unterscheiden in unveränderliche und sich verändernde, sogenannte polymorphe Viren.
<i>Würmer</i>	Würmer sind kleine selbstständige Programme. Im Gegensatz zu Viren benötigen sie kein Wirtsprogramm. Sie und ihre Kopien sind in der Lage, sich selbst zu reproduzieren. Würmer breiten sich insbesondere über Netzwerke und mittels E-Mails aus.
<i>Trojanische Pferde</i>	Trojanische Pferde sind Programme, die unbemerkt vom Nutzer unerwünschte Aktionen ausführen. Der Nutzer nimmt dabei nur den Teil der Programmaktivitäten wahr, die für ihn bestimmt sind. Versteckte Funktionen können beispielsweise im Versand vertraulicher Dateien oder Informationen, z. B. der Benutzerkennung und des Passworts, an Unbefugte bestehen.
<i>Virens Scanner</i>	Um Rechner vor Computerviren zu schützen, setzen Unternehmen Virens Scanner bzw. Viren-Suchprogramme ein. Sie durchsuchen Programme nach der ihnen bekannten Malware in Form von Computerviren, Makroviren, Würmern und trojanischen Pferden. Hierzu nutzen sie u. a. eine Datenbank mit den Charakteristika der Computerviren, z. B. in Form der Virenkennung oder von Byte-Mustern. Außerdem verfügen sie über eine Liste derjenigen Dateien, die auf Viren zu durchsuchen sind. Hierzu gehören insbesondere ausführbare Programme, z. B. Dateien mit der Endung .exe oder .com. Tests zeigen, dass Virens Scanner eine unterschiedliche Erkennungsrate für Viren haben, die üblicherweise unterhalb von 100 % liegt. Dies kann die Kombination von Virens Scannern unterschiedlicher Herstellern sinnvoll machen. Hierbei verfügen z. B. zentrale Server über den Virens Scanner eines anderen Herstellers als die dezentralen PCs.
<i>Zeitnahe Aktualisierung</i>	Wegen der kontinuierlichen und dynamischen Entstehung neuer Viren verlieren Virens Scanner, die nicht aktualisiert werden, im Laufe der Zeit an Wirksamkeit, da sie nur jene Computerviren bzw. Virensignaturen kennen, die zu dem Zeitpunkt bekannt waren, an dem der Virens Scanner erstellt wurde. Außerdem können auch Virens Scanner

Sicherheitslücken aufweisen. Die Schutzsubjekte Virens Scanner sind – wie bereits erläutert – somit gleichzeitig Schutzobjekte. Aus den genannten Gründen müssen Virens Scanner fortlaufend, sehr zeitnah (täglich) und möglichst automatisiert aktualisiert werden. Damit Virens Scanner ihren Zweck möglichst gut erfüllen können, muss der jeweilige Hersteller die Signaturen neuer Malware sehr kurzfristig bereitstellen.

Eine Herausforderung für Computervirens Scanner stellt der Schutz vor mutierender und neuer Malware sowie den damit verbundenen Zero-Day-Attacken oder Before-Zero-Day-Attacken dar. Für diese Malware sind zum Zeitpunkt eines möglichen Angriffs noch keine Signaturen bekannt. Zero-Day-Attacken nutzen eine Sicherheitslücke zum Zeitpunkt ihres Bekanntwerdens aus. Before-Zero-Day-Attacken nutzen noch nicht allgemein bekannte Sicherheitslücken aus. Dem versuchen Hersteller von Virensuchprogrammen entgegenzuwirken, indem sie beispielsweise heuristische Verfahren einsetzen, welche Programme auf verdächtige Programmsequenzen hin untersuchen und die Wahrscheinlichkeit einer Infektion bewerten.

Virens Scanner können auf zwei Arten genutzt werden: transient (on demand), d. h. sie werden durch individuellen Aufruf des Benutzers gestartet, oder resident, d. h. sie werden beim Start des Rechners in den Speicher geladen und verrichten ihre Aufgabe im Hintergrund ohne Zutun des Benutzers. Wegen des kontinuierlichen Schutzbedarfs setzen Unternehmen auf die residente Nutzung.

*Transiente und
residente
Nutzung*

9.5.23.6 Security Appliance

Security Appliances, für die das Marktforschungsunternehmen IDC den Begriff Unified Threat Management (UTM) prägte, vereinigen eine Vielzahl von Schutzfunktionalitäten in sich. Die Funktionalitäten dieser integrativen Lösungen reichen vom Firewall über Viren-, Spyware- und Spamschutz sowie Phishing- und Content-Filter bis hin zu Intrusion Detection and Prevention. Je nach Ausstattung unterstützen sie darüber hinaus Deep Packet Inspection, Portscan-Detection, NAT, Port Masquerading und Load Balancing.

9.5.23.7 Automatisierte biometrische Systeme

Der Begriff Biometrie entstammt dem griechischen bios (βίος) = Leben und metrein (μετρεῖν) = messen. Biometrie befasst sich dementsprechend mit der quantitativen Messung biometrischer, vor allem menschlicher Merkmale. Außerhalb der Biologie und Medizin geht es bei der Biometrie insbesondere um die Nutzung biometrischer Merkmale zur Identifizierung oder Verifizierung von Personen, u. a.

Biometrie

bei der Grenzkontrolle, der Zutrittskontrolle zu Hochsicherheitsbereichen, z. B. Rechenzentren, und der Zugangskontrolle zu Computersystemen.

Biometrische Systeme können physiologische oder verhaltensbasierte Merkmale nutzen. Physiologische Merkmale sind angeboren und willentlich nicht veränderbar, sofern wir Operationen und Verletzungen ausschließen.

*Automatisierte
biometrische
Identifizierung
und
Authentifizierung*

Automatisierte biometrische Systeme [75] (biometric system) nutzen physiologische oder verhaltensbasierte Merkmale zur Identifizierung einer Person oder zu deren Authentifizierung bzw. Verifizierung:

- Automatisierte biometrische Identifikationssysteme (Automated Biometric Identification System) (ABIS) finden eine Person anhand deren biometrischen Merkmals aus einer Menge gleichartiger biometrischer Merkmale von N Personen heraus. Das biometrische System führt hierzu einen 1:N-Vergleich (One-To-Many-Matching {O2M}) durch. ABIS geben Antwort auf die Frage: Wer ist diese Person? Etwas detaillierter betrachtet lautet die Frage: Gehört diese Person zu den bei mir gespeicherten Personen und wenn ja, welche ist es? Je größer der Datenbestand ist, desto umfangreicher wird die Suche und desto länger dauert sie.
- Automatisierte biometrische Authentifizierungssysteme (Automated Biometric Authentication System) (ABAS) vergleichen das aktuelle biometrische Merkmal einer Person mit dem für diese Person gespeicherten biometrischen Merkmal. Das biometrische System führt hierzu einen 1:1-Vergleich (One-To-One-Matching {O2O}) durch. ABAS geben Antwort auf die Frage: Ist die Person diejenige, die zu sein sie vorgibt? Dieser Vergleich ist deutlich weniger aufwändig als der bei Identifikationssystemen und daher prinzipbedingt schneller.

*Physiologische
Merkmale*

Biometrische Systeme können die folgenden physiologischen Merkmale nutzen: Muster, z. B. Iris- (Regenbogenhaut), Retina- (Netzhaut-), Handlinien-, Fingerlinien- (Fingerabdruck), Fingerven-, Handvenenmuster, bioelektrische Signale, oder die Geometrie, wie z. B. die Kopf-, Gesichts-, Ohr-, Hand- oder Zweifingergeometrie. Ferner können das thermische Gesichtsbild, das Aussehen (Foto) und nicht zuletzt die menschliche DNA (genetischer Fingerabdruck) zum Einsatz kommen.

*Verhaltens-
basierte
Merkmale*

Darüber hinaus lässt sich auch das Verhalten einer Person zur Identifizierung oder Authentifizierung heranziehen. Ein altbekanntes Verfahren, persönliches Verhalten zur Authentifizierung zu nutzen, ist die Unterschrift. Wird die Unterschrift auf einer Schreibunterlage mit Drucksensoren geleistet, so lassen sich neben der Form der Unter-

schrift gegebenenfalls auch die Schreibgeschwindigkeit und der Druck des Stiftes überprüfen. Weitere Verhaltensmuster ergeben sich aus dem Stimmprofil, den Lippenbewegungen, dem Gang und dem Tippverhalten an einer Tastatur. Diese Verfahren nutzt auch der Mensch, indem er telefonische Gesprächspartner an der Stimme oder Bekannte von weitem am Gang erkennt.

Voraussetzungen für die Nutzbarkeit eines biometrischen Merkmals zur Identifizierung oder Authentifizierung sind seine:

*Nutzbarkeit
biometrischer
Merkmale*

- Universalität,
- Einzigartigkeit bzw. Einmaligkeit,
- Unveränderbarkeit,
- Beständigkeit und
- Messbarkeit.

Dadurch, dass diese Voraussetzungen in der Regel nicht alle zu 100 % erfüllt sind, ergeben sich Risiken. Betrachten wir die Forderung nach Universalität. Sie bedeutet, dass das biometrische Merkmal bei jedem Menschen vorhanden sein muss. Genetisch oder krankheitsbedingt können jedoch z. B. Fingerlinien (Fingerabdruck) bei Menschen in seltenen Fällen fehlen. Wie sieht es nun mit der Einmaligkeit aus?

Die Forderung nach Einzigartigkeit bzw. Einmaligkeit ist bei biometrischen Merkmalen nach meinem Kenntnisstand nicht gegeben. Die genutzten biometrischen Merkmale können zwar rechnerisch üblicherweise eine Vielzahl unterschiedlicher Ausprägungen annehmen. Die sehr hohe empirische Seltenheit eines identischen Merkmals ist teilweise ebenfalls belegt, z. B. bei Fingerabdrücken. Gleichzeitig ist ihre Ausprägung zufällig. Bei exakt identischem biometrischen Merkmal lautet die Aussage daher, dass die Person „sehr wahrscheinlich“ mit der identisch ist, deren Referenz zugrunde gelegt wurde.

Die rechnerisch ermittelte Unterscheidbarkeit sollte anhand einer entsprechend großen Anzahl von Personen sowie an eineiigen Zwillingen verifiziert sein. Hierbei ist nicht nur die qualitative Unterschiedlichkeit, sondern auch der Grad der Unterschiedlichkeit wichtig.

Sind angeborene Merkmale unveränderbar? Auch dies ist nicht zu 100 % gegeben, wenn wir an (plastische) Operationen denken.

Die Beständigkeit eines biometrischen Merkmals im Lebenslauf eines Menschen ist ein weiterer Aspekt. Um sie beurteilen zu können, sind Langzeiterfahrungen erforderlich. Der Fingerabdruck ist hierbei mit über 100jähriger Geschichte und dem Einsatz in der Kriminalistik

führend. Mit verschiedenen anderen Merkmalen liegen keine Langzeiterfahrungen über mehrere Jahrzehnte vor.

Die Messbarkeit eines biometrischen Merkmals ist oftmals technisch und nutzungsbedingt eingeschränkt. Identifikations- und Authentifizierungsvorgänge sollen innerhalb einer oder weniger Sekunden durchgeführt sein. Da eine entsprechende Prozessorleistung für einen 100 %igen Vergleich des kompletten Merkmals verschiedentlich nicht ausreicht, beschränken biometrische Systeme den Vergleich auf charakteristische Elemente. Dies reduziert die rechnerisch ermittelte hohe Unterscheidbarkeit des biometrischen Merkmals in der Regel auf technisch und nutzungsbedingt mögliche Werte.

Außerdem sind z. B. Position, Neigung, Winkel, Druck und Ausleuchtung potenzielle Parameter, in denen sich die aktuell erfassten Daten des jeweiligen biometrischen Merkmals von den Referenzdaten (template) unterscheiden können. Daher müssen Algorithmen die aktuellen Daten so transformieren, dass ein Vergleich möglich ist. Hierdurch entstehen Abweichungen vom Original. Um eine Identifizierung oder Authentifizierung zu ermöglichen, ist eine Akzeptanzschwelle festzulegen, bis zu der das System Abweichungen zwischen Referenzdaten und aktuell erhobenen Daten des Merkmals toleriert.

*Falschakzeptanzrate (FAR),
Falschrückweisungsrate (FRR)*

Hieraus resultieren die Falschakzeptanzrate (False Acceptance Rate {FAR}) und die Falschrückweisungsrate (False Rejection Rate {FRR}). Sie geben an, wie oft statistisch eine Person fälschlicherweise akzeptiert bzw. zurückgewiesen wird. Falschrückweisungsrate sind in gewissem Umfang als „Schönheitsfehler“ hinnehmbar, da ein erneuter Scan-Vorgang üblicherweise erfolgreich ist. Kritisch ist jedoch die FAR, da das System hierdurch Unberechtigte als Berechtigte ansieht und zulässt.

Die FARs technischer Systeme liegen derzeit meist deutlich unter der rechnerisch möglichen Unterscheidbarkeit eines biometrischen Merkmals. Im August 2005 veröffentlichte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) die Studie BioP II. Hierbei ließen sich für biometrische Systeme mit optischen Fingerabdruck-Scannern FARs von 1:100.000 bei einer FRR von 2 % erreichen. Im Vergleich zur Gesichts- und Iriserkennung wies die Fingerabdruckerkennung bei gleicher FAR die geringste FRR auf.

Funktionsweise

Automatisierte biometrische Systeme nehmen zu Beginn die Daten des biometrischen Merkmals einer Person auf. Diese Phase heißt Registrierung, englisch enrolment. Als Ergebnis liegen die Referenzdaten (template) vor. Im Betrieb vergleichen biometrische Systeme die aktuell ermittelten biometrischen Daten mit den Referenzdaten.

Ein automatisiertes biometrisches System besteht aus folgenden Komponenten:

- einem Sensor, der das biometrische Merkmal erfasst (capture). Er stellt die Verbindungsstelle zwischen Mensch und System dar
- einem Speicher, in dem die Referenzdaten abgelegt sind
- einem Prozessor, der die vom Sensor gelieferten Daten vorverarbeitet und die charakteristischen Daten des biometrischen Merkmals extrahiert (extract).
Anschließend vergleicht (match) er die aktuell ermittelten Daten mit den gespeicherten.
Entsprechend der eingestellten bzw. gespeicherten Akzeptanzschwelle entscheidet (decide) er, ob eine Übereinstimmung vorliegt oder nicht.
Das Ergebnis gibt er aus.

Das derzeit bekannteste und verbreitetste biometrische Merkmal ist der Fingerabdruck. Viele Menschen sind ihm zwar nicht im wahren Leben, aber dafür in Kriminalromanen oder Filmen begegnet, in denen Fingerabdrücke im Rahmen der Daktyloskopie zur Identifizierung von Tätern und zum Ausschluss Unschuldiger genutzt werden. Gegen Ende des Jahres 2007 sollen Fingerabdrücke auch im deutschen elektronischen Reisepass (ePass) gespeichert werden.

Fingerabdruck

Fingerabdrucksensoren (Fingerprint Scanner) lassen sich unterscheiden in optische und Festkörpersensoren (solid-state). Darüber hinaus existieren hochfrequente, drucksensitive, thermische und Ultraschall nutzende Sensoren.

Fingerabdruck-sensor

Fingerabdrucksensoren sind ausgeführt als Flächensensoren und Streifensensoren. Bei Flächensensoren legt der Nutzer seinen Finger unbeweglich entweder direkt auf die Sensorfläche auf (touch) oder hält ihn darüber. Bei Streifensensoren zieht er seinen Finger über den Sensor (sweep).

*Flächensensor,
Streifensensor*

Weit verbreitet sind kapazitive Sensoren, die auch in handelsüblichen Notebooks, USB-Memory-Sticks, externen Festplatten sowie USB-Token zum Einsatz kommen. Die Bequemlichkeit, sich z. B. keine Passwörter mehr merken zu müssen, ist aus Anwendersicht einer der Vorteile derartiger Systeme. Er führt dort zu hoher Akzeptanz.

Ein weiteres Merkmal biometrischer Systeme ist die Täuschungsanfälligkeit bzw. Überlistbarkeit des Systems, z. B. durch die reine oder aufgesetzte Attrappe eines Fingerabdrucks oder einer Iris oder auch den Mitschnitt einer Stimme.

Täuschungs-anfälligkeit

Darüber hinaus empfiehlt sich – wie bei jedem System – eine Chancen-Risiko-Betrachtung, z. B. im Hinblick auf Bedrohungen und Schutzmaßnahmen bei der Übertragung, der Verarbeitung, der Speicherung und der Nutzung. Ebenfalls zu berücksichtigen sind Aspekte des Datenschutzes und der Gleichbehandlung, in Deutschland beispielsweise in Form des Allgemeinen Gleichbehandlungsgesetzes (AGG).

Datenschutzaspekte ergeben sich daraus, dass z. B. über Iriserkennung und bioelektrische Signale Informationen erfasst werden, die prinzipiell Rückschlüsse auf den Gesundheitszustand der Person ermöglichen.

Das Thema Gleichbehandlung spielt eine Rolle, wenn ein biometrisches Merkmal bei einzelnen Personen nicht in der Ausprägung vorhanden ist, wie es zur Nutzung des biometrischen Systems erforderlich wäre. Bei Bürotätigen liegt der Anteil unzureichend ausgeprägter Fingerabdrücke bei ca. 1 %. Für diese Personen sind – ebenso wie für den Fall größerer Verletzungen – Alternativsysteme erforderlich.

*Betriebsrisiken
bzw.
operationelle
Risiken*

Die Verantwortung für den ordnungsgemäßen Betrieb eines biometrischen Systems liegt bei dessen Betreiber. Speichert dieser die biometrischen Referenzdaten, so ist er für deren Sicherheit verantwortlich, ähnlich wie bei Passwörtern. Während sich korruptierte Passwörter jedoch verändern lassen, ist dies bei biometrischen Merkmalen nicht der Fall. Hieraus können Benutzer potenzielle Haftungsansprüche ableiten, obwohl sich aus dem gespeicherten Datensatz in der Regel nicht das komplette Original rekonstruieren lässt. Sicherheitsmaßnahmen bestehen in der Verschlüsselung sowie der getrennten Speicherung von Referenzdaten und zugehörigem Benutzer.

Im Gegensatz zu Passwörtern, bei denen das Ergebnis der Überprüfung „richtig“ oder „falsch“ ist, besitzen biometrische Systeme einen Toleranzbereich, innerhalb dessen das biometrische Merkmal als übereinstimmend anerkannt wird. Dementsprechend lautet das Ergebnis eines biometrischen Systems, dass es eine Übereinstimmung im Rahmen der gewählten Vergleichselemente/-punkte und der Toleranzvorgaben festgestellt hat, sie also „sehr wahrscheinlich“ ist. Streitet ein Nutzer ab, ein System zu einem Zeitpunkt genutzt zu haben, zu dem das System ihn als Nutzer identifiziert hatte, kann der Betreiber den Nachweis des Gegenteils nur im Rahmen der FAR erbringen. Hinzu kommen Bedrohungen aufgrund von Angriffen in Form des „biometric hacking“, wie der Autor derartige Angriffsszenarien bezeichnet.

Auch beim „biometric hacking“ [75] bietet das Prinzip der Pfadanalyse eine systematische Vorgehensweise zur Ermittlung von Angriffszielen, Angriffsszenarien und Abwehrmaßnahmen. Angriffsziele bilden das biometrische Merkmal selbst, der Sensor, der Algorithmus, die Übertragungsstrecken, die Speichereinheiten, die Referenz- und Benutzerdaten, die Akzeptanzschwelle und die Verarbeitungseinheiten. Angreifer zielen darauf ab, Komponenten zu täuschen, z. B. den Sensor durch eine Attrappe, oder Daten zu manipulieren oder zu stehlen.

*„biometric
hacking“*

Wesentliche Sicherheitsmaßnahmen bestehen z. B. in der „fehlerfreien“ Lebenderkennung, der sicheren gegenseitigen Authentisierung und Authentifizierung der beteiligten Komponenten und der Erkennung und Verhinderung von „Replay“-Attacken. Weitere Maßnahmen sind der Zugangs- und Zugriffsschutz, z. B. zur Verhinderung von Denial-of-Service-Attacken, die der Autor in diesem Kontext als Denial-of-Authentication-Attacken bezeichnet, sowie der sicher verschlüsselten Übertragung und Speicherung von Daten.

*Abwehr-
maßnahmen*

Zur Reduzierung von Bedrohungen durch Angriffe auf Übertragungsstrecken und Komponenten dienen beim Fingerabdruck sicher gekapselte Chipkarten. Bei ihnen befinden sich zum einen die Referenzdaten auf dem Chip und zum anderen erfolgt der Verifizierungsvorgang im Chip. Dieser Vorgang heißt „match on device“. Einen Schritt weiter gehen USB-Token, die ein „authentication on device“ ermöglichen. Sie verfügen über einen Chip, in dem die Referenzdaten gespeichert sind und der Verifizierungsvorgang abläuft, sowie über einen im Token integrierten Fingerabdrucksensor.

Aufgrund der derzeit technisch erreichbaren Genauigkeit und Angriffssicherheit biometrischer Verfahren sollte ab einem bestimmten Schutzbedarf eine Zweifaktorauthentisierung zum Einsatz kommen, beispielsweise als Kombination aus einem USB-Token und dem Fingerabdruck. Für die Übereinstimmung der jeweiligen Sicherheitsanforderungen mit dem erreichbaren Sicherheitsniveau müssen die Sicherheitsverantwortlichen sorgen. Sicherheitsüberlegungen sind dementsprechend ab der ersten Idee für ein solches System und dann entlang dem Lebenszyklus zu berücksichtigen.

Unzureichende Lebenderkennung stellt bei biometrischen Verfahren eine latente Bedrohung dar, zum einen hinsichtlich der körperlichen Unversehrtheit des Nutzers durch Angreifer, zum anderen im Hinblick auf die Überlistung des Systems. Dies umso mehr, wenn sich aufgrund der Nutzung ein geeigneter Fingerabdruck auf der Karte oder dem Token befindet.



Akzeptanz biometrischer Verfahren

Die Vielzahl technischer Geräte, die mit einem Fingerabdrucksensor ausgestattet sind, aber auch der ePass mit der für Ende 2007 geplanten Speicherung von Fingerabdrücken, zeigt die zunehmende Akzeptanz biometrischer Verfahren. Einer Studie des Ponemon Institute zufolge, die aus dem Jahr 2006 stammt, befürworten 69 % der befragten Europäer die Biometrie. Weltweit liegt demzufolge die Akzeptanz für die Stimmerkennung knapp vor der des Fingerabdrucks. Vanson Bourne führte 2006 eine Umfrage durch, wonach 84 % der Europäer bereit wären, sich bei Auslandsreisen einem Fingerabdruck- oder Netzhaut-Scan zu unterziehen.

*Trends zum
Multi..., etc.*

Stand 2007 zeichnet sich der Trend zur Zwei- und Mehrfaktor-identifizierung bzw. -authentifizierung ab. Erkennbar ist dies beispielsweise an japanischen Scheckkarten, die Finger- oder Handvenenmuster speichern, Chipkarten, die den Fingerabdruck speichern und den „match on device“ durchführen, sowie USB-Token mit Fingerabdrucksensor und „authentication on device“.

Multispektrale und multimodale Verfahren liegen ebenfalls im Trend. Multispektrale Verfahren gelangen beim Fingerabdruck-Scan zum Einsatz. Hierbei erzeugt der Sensor bei unterschiedlichen Wellenlängen vom sichtbaren bis zum infrarotnahen Licht Abbildungen des Fingerabdrucks. Die so gewonnenen Daten von der Fingeroberfläche und Bereichen unterhalb der Hautoberfläche ermöglichen es, einerseits eine Vielzahl von Attrappen zu erkennen und andererseits selbst bei nassen, trockenen und schmutzigen Fingern Abdrücke zu nehmen, die sich weiter verarbeiten lassen.

Multimodale Verfahren verwenden mehrere unterschiedliche biometrische Merkmale zur Identifizierung oder Authentifizierung. Hierzu zählen u. a. die Iris-Gesichtserkennung, die Iris-Fingererkennung und die Gesichts-Fingererkennung. Das deutsche BSI erwartet hierbei aufgrund von Untersuchungen aus dem Jahr 2005 Fehlerraten, die um ca. eine Zehnerpotenz niedriger liegen als bei den monomodalen Verfahren.

Bei Fingerabdruck-Scannern läuft der Trend in Richtung höherer Auflösung von derzeit 500 ppi (pixel per inch) hin zu 1.000 ppi.

EU-Projekte

Darüber hinaus fördert die EU das Projekt 3D-Face zur Entwicklung dreidimensionaler Gesichtserkennungssysteme für die Grenzkontrolle. Das Projekt unter der Projektleitung von Sagem Défense Sécurité, Frankreich, startete im April 2006.

Einsatzgebiete

Die Einsatzgebiete automatisierter biometrischer Systeme reichen von der Grenzkontrolle und Überwachung über die Zutrittskontrolle bis hin zur Zugangskontrolle und zur Authentisierung bei Finanz-

transaktionen. Ziele derartiger Systeme sind die Erhöhung der Wirtschaftlichkeit und der Sicherheit. Zur Zutrittskontrolle im Einsatz sind – teilweise auch bei Banken – beispielsweise Systeme zur dreidimensionalen Gesichtserkennung, zur Iris- und zur Fingerabdruckerkennung.

Die Stimmerkennung verwenden Unternehmen beim Telefonbanking und im Self Service, z. B. innerhalb eines Unternehmens zur Passwortrücksetzung. Handelsunternehmen nutzen die Fingerabdruckerkennung zum Bezahlen, japanische Banken setzen Finger- oder Handvenenerkennung in Kombination mit der Scheckkarte zum Abheben an Geldautomaten ein. Handys und PDAs mit integrierter Kamera können per Iriserkennung geschützt sein. Notebooks, USB-Sticks und mobile Festplatten können mit Fingerabdrucksensoren ausgestattet sein.

9.5.24 Infrastruktur

Die Infrastruktur eines Unternehmens umfasst Gebäude, Haustechnik, Räumlichkeiten, Maschinen, Anlagen, Versorgungseinrichtungen und weitere Schutzsubjekte. Baupläne sowie Pläne der Verkabelung und Verrohrung geben den Überblick über die jeweilige konkrete Infrastruktur. Zu diesen Plänen gehören Raumpläne mit deren jeweiliger Infrastruktur, Lagepläne für Hydranten, Verrohrungspläne für Gas, Wasser, Heizung und Raumlufte sowie Trassenwege- und Trassenbelegungs- bzw. Kabelpläne für Strom und Daten.

Zur Versorgungstopologie gehört seitens des Facility Management die Aufstellung, welche Verbraucher an die USV und welche an die NEA angeschlossen sind. An USV und/oder NEA sind – abhängig von den Sicherheitsanforderungen – in der Regel folgende Ressourcen angeschlossen: die sicherheitsrelevanten Informationssysteme, die TK-Anlage, das Zutrittskontrollsystem, die Gefahren-, Brand-, Einbruch- und Wassermeldeanlage, geschäfts- und sicherheitskritische Anlagen und Arbeitsplätze, die Notbeleuchtung, die Klimaanlage für die Serverräume bzw. das Rechenzentrum und die Fahrstühle.

Für jede Ressource legen die Verantwortlichen fest, welche Sicherheitselemente für die Prävention, Detektion, Reaktion, Restauration und Verifikation vorgesehen sind. Das folgende überblicksartige und ausschnittsweise Beispiel veranschaulicht dies.

Thema		Betriebs- sicherheit	Angriffs- sicherheit	Typ, Thema
Ab V-Klasse		Ab S-Klasse		
Versorgungseinrichtungen				
Elektro	Leitungsführung zum Haus redundant und räumlich getrennt	4		P,T
	Netzanbindung redundant und räumlich getrennt	4		P,T
	Hausanschlussschächte gesichert	4		P,T
	Leitungsführung inhouse redundant und räumlich getrennt	3		P,T
	Unterbrechungsfreie Stromversorgung (USV)			P,T
	VFI-USV (s.a. „Online“-USV)	2		
	VFD-USV (s.a. „Offline“-USV)			
	Netzersatzanlage (NEA)	3		P,T
	Überspannungsschutz	3		P,T
	...			
Gebäude und Räumlichkeiten				
Technikräume/Serverräume	Baulicher Einbruchschutz	2		P,T
	Einbruchmeldeanlage (EMA)	3		D,T
	Baulicher Brandschutz	2		P,T
	Organisatorischer Brandschutz	2		P,O
	Brandmeldeanlage (BMA)	3		D,T
	Baulicher Wasserschutz	3		P,T
	Wassermeldeanlage (WMA)	3		D,T
	Zutrittskontrollsystem (ZKS)	2		P,T
	...			
...				
...				
...				

Legende: V-Klasse = Verfügbarkeitsklasse, S-Klasse = Sicherheitsklasse
 Klasse: 1 = niedrigste Klasse, ... 4 = höchste Klasse
 Typ: P = Prävention, D = Detektion/Alarmierung/Meldung, R = Reaktion, V = Verifikation
 Thema: P = Prozess, T = Technologie, O = Organisation, M = Mitarbeiter, Personal

9.5.25 Dokumente

Unternehmen verfügen über spezifische Methoden und Verfahren. Diese sollten in einem Überblick dokumentiert sein. Hierzu gehört die Angabe ihres Einsatzgebietes, Zusammenspiels mit anderen Verfahren sowie ihre Bedeutung für das Unternehmen.

Den Mitarbeitern eines Unternehmens sollten jene Dokumente bekannt und in der aktuellen Version zugreifbar sein, die für ihre Aufgabe relevant sind. Wie aus der DIN EN ISO 9000ff. bekannt ist, sind Schemata für die eindeutige Identifikation von Dokumenten, für die Kennzeichnung ihres Status und ihrer Aktualität erforderlich. Die Dokumentenarchitektur stellt dar, in welchem hierarchischen Verhältnis Dokumente zueinander stehen, wie sie zusammenspielen und welchen Konventionen ihre Namen und ihr Layout gehorchen. Umgekehrt formuliert deuten z. B. undatierte oder nicht eindeutig gekennzeichnete Dokumente auf Optimierungspotenziale bei Organisation und Ordnungsmäßigkeit hin.

9.5.26 Personal

In Unternehmen gibt es Funktionen und Rollen. Diesen sind Qualifikationsprofile (skill profile) zugeordnet. Hieraus ergibt sich der Zielzustand der Qualifikationsarchitektur. Im Sicherheits-, Kontinuitäts- und Risikomanagement finden sich z. B. die Rollen Sicherheits-, Kontinuitäts- und Risikomanager sowie Administratoren und Datenschutzbeauftragte mit entsprechenden Qualifikationsprofilen und entsprechender Sicherheitseinstufung.

Den verschiedenen in einem Unternehmen definierten Funktionen und Rollen sind Personen zugeordnet. Diese Personen besitzen Qualifikationsprofile, die mehr oder weniger deckungsgleich mit den geforderten Profilen sind. Führungskräfte sind im Rahmen des Personalmanagements gefordert, die aktuellen oder mittelfristigen Qualifikationslücken bzw. -bedarfe ihrer Mitarbeiter aufzuzeigen und Maßnahmen zu deren Beseitigung zu vereinbaren. Ziel ist die weitgehende Deckungsgleichheit zwischen Ist- und Soll-Qualifikationsarchitektur.

9.5.27 Organisation im Überblick

Über die Sicherheitspyramide und deren Ebenen sowie die Prozesse, die Ressourcen und das Sicherheitsschalenmodell ergeben sich Aufgaben. Für diese sind Verantwortlichkeiten in Form von Rollen, z. B. Chief ICT Security Officer (CISO), Chief ICT Continuity Officer (CICO), Chief Compliance Officer (CCO), Chief Business Continuity

Officer (CBCO) und Datenschutzbeauftragter, sowie Teams, z. B. der Lenkungsausschuss IT-Sicherheit, das Computer Security Incident Response Team (CSIRT) und der Krisenstab, festzulegen. Die dazugehörigen Aufgaben beinhalten neben der Entwicklung auch die kontinuierliche Pflege des jeweiligen Aufgabenobjektes. Für diese Funktionen bzw. Rollen sind im Hinblick auf das Thema Sicherheit folgende Beschreibungen zu erstellen:

- Funktions-/Rollenbeschreibung
- Qualifikationsprofil
- Berichtsweg
- Kommunikationspfade

Über eine Matrix lassen sich den jeweiligen Aufgaben die dazugehörigen Rollen zuordnen.

9.5.28 Lebenszyklus im Überblick

Die vorangegangenen Kapitel betrachteten die Prozesse, die Ressourcen und die Organisation. Zusätzlich ist deren Lebenszyklus zu berücksichtigen. Hierzu wird für die einzelnen Phasen im Lebenszyklus, wie z. B. die Konzeptions-, Entwicklungs-, Betriebs- und Außerbetriebnahmephase, beschrieben, welche PROSim-Elemente wie zu berücksichtigen und welche Schnittstellen zu bedienen sind. Hierbei ist u. a. zu definieren, welche Technologien, z. B. Entwicklungstools, Hilfsmittel und Standards zum Einsatz kommen, wie die Organisation aussieht und welches Personal mit welchem Wissen und welchem Sicherheitsniveau einzusetzen sind.

9.6 Hilfsmittel Sicherheits- und Risikoarchitekturmatrix

Die vorangegangenen Kapitel haben gezeigt, dass Sicherheitselemente für eine breite Themenpalette aufgestellt werden sollten. Um hierfür den Überblick zu er- und behalten, empfiehlt es sich, z. B. eine Architekturmatrix anzulegen.

Thema		P	R	O	Typ
Leistungsmanagement					
	Leistungsvereinbarungen	Z ☹	Z ☹	Z ☹	
	Externe Leistungserbringung (Service-Geber)	O ☺	O ☺	O ☺	
	...				
...					
Kontinuitätsmanagement					
	Lage und Umfeld des Gebäudes	Z ☹	Z ☹	Z ☹	
	Externe Versorgung	Z ☹	Z ☺	Z ☺	

Thema	P	R	O	Typ
Gebäude und Infrastruktur	Z ☺	Z ☺	Z ☺	
...	Z ☺	Z ☺	Z ☺	
Datensicherung	Z ☺	Z ☺	Z ☺	
...				
Notfall- und Katastrophenvorsorgeplanung	Z ☺	Z ☺	Z ☺	
Securitymanagement				
Objektschutz	O ☺	O ☺	O ☺	
Zufahrtsschutz	O ☺	O ☺	O ☺	
Zutrittsschutz	Z ☺	Z ☺	Z ☺	
Zugangsschutz	Z ☺	Z ☺	Z ☺	
...				
... Legende: Überschrift: P = Prozess, R = Ressource, O = Organisation Anforderung: z = zwingend erforderlich, o = optional, Status: ☺ = noch nicht geplant, ☺ = bereits konzipiert, ☺ = eingeführt				

Die Architekturmatrix gibt zu den verschiedenen Themenfeldern überblicksartig und zusammenfassend an, ob jeweils ein Sicherheitselement zwingend erforderlich (z) oder optional (o) ist. Dies ermöglicht einerseits einen schnellen Überblick über die geforderten Sicherheitselemente. Zusätzlich kann durch eine farbliche und/oder symbolische Kennzeichnung festgestellt werden, ob dieses Element noch nicht geplant (☺), bereits konzipiert (☺) oder eingeführt (☺) ist und wo es Bereiche gibt, die noch auszufüllen sind. Der Detaillierungsgrad der Auflistung und der Kennzeichnung lässt sich bedarfsorientiert weiter verfeinern oder in weiteren Dokumenten abbilden. Ein prinzipielles und auszugsweises Beispiel zeigt die Tabelle.

Die Sicherheitsarchitektur bildet das zentrale Element auf dem Weg zur ganzheitlichen Umsetzung der Sicherheitsanforderungen. Sie untergliedert sich in die Ebenen zusammenfassende Sicherheitsanforderungen, prinzipielle Bedrohungen, Strategien und Prinzipien zur Erhöhung des Sicherheitsniveaus. Außerdem finden sich hier die Sicherheitselemente für die Betriebs- und Angriffssicherheit sowie die Kontinuität (s. a. Klassen-Maßnahmen-Matrix).

Die zusammenfassenden Sicherheitsanforderungen dienen dazu, die Wirtschaftlichkeit und Effizienz des Sicherheits-, Kontinuitäts- und Risikomanagements durch Klassenbildung zu erhöhen. Für jedes Sicherheitskriterium lassen sich Klassen bilden, z. B. Verfügbarkeitsklassen und Vertraulichkeitsstufen, für die in der Folge standardisierte Sicherheitsrichtlinien sowie darauf aufbauende Konzepte und Maßnahmen gelten.

*Kernelement
Sicherheits-
architektur*

*Zusammen-
fassende
Sicherheits-
anforderungen*

9.7 Zusammenfassung

<i>Prinzipielle Bedrohungen</i>	Die prinzipiellen Bedrohungen verschaffen einen Überblick über die Vielfalt der möglichen Szenarien. Diese Übersicht ermöglicht es, Bedrohungen zu Gruppen zusammenzufassen (clustern), denen sich z. B. im Hinblick auf die Behebung Richtlinien sowie standardisierte Konzepte und Maßnahmen zuordnen lassen.
<i>Strategien und Prinzipien</i>	Die Strategien und Prinzipien zur Erhöhung des Sicherheitsniveaus und zur Optimierung des Risikoportfolios unterstützen das systematische, zielorientierte und effiziente Herangehen an Sicherheits- und Risikothematiken. So hilft z. B. die Pfadanalyse, Sicherheitslücken und fehlende Redundanzen zu entdecken.
<i>Sicherheits-elemente, Prozesse, Ressourcen und Organisation</i>	Ausgehend von den Anforderungen, den prinzipiellen Bedrohungen sowie den Sicherheitsstrategien und -prinzipien werden Sicherheits-elemente zur Erhöhung der Betriebs- und Angriffssicherheit entwickelt. Hierbei werden die Prozesse und Ressourcen des ITK-Lebenszyklus und die daraus resultierenden Anforderungen und Ergebnisse berücksichtigt. Die Begleitprozesse (Management-disziplinen) erstrecken sich vom Konformitäts-, Datenschutz- und Risikomanagement über das Leistungs-, Finanz-, Projekt- und Qualitätsmanagement bis hin zum Ereignis-, Problem-, Änderungs-, Release-, Konfigurations-, Lizenz-, Kapazitäts-, und Wartungsmanagement. Sie umfassen ferner das Kontinuitäts- und Securitymanagement sowie das Architektur-, Innovations- und Personalmanagement. Die sicherheitsrelevanten Ressourcen werden ebenso erhoben, wie die Sicherheitsorganisation.
<i>Lebenszyklus</i>	Die Prozesse und Ressourcen werden später in die Phasen des Lebenszyklus der ITK-Systeme integriert, die sich über die Konzeptions-, Entwicklungs- und Betriebs- bis hin zur Außerbetrieb-nahme-phase erstrecken.
<i>Architektur-matrix</i>	Die Sicherheitselemente können in einer Architekturmatrix abgebildet und als zwingend erforderlich oder optional gekennzeichnet werden. Eine entsprechende Farbgebung (Ampelfarben) macht sichtbar, in welchem Umsetzungsstadium (geplant, konzipiert, umgesetzt) sie sich jeweils befinden.

10 Sicherheitsrichtlinien/-standards – Generische Sicherheitskonzepte

Das vorangegangene Kapitel beschäftigte sich mit der Sicherheitsarchitektur und legte die Sicherheitselemente fest, mit denen die Sicherheitsziele erreicht werden sollen.

Die im Folgenden behandelte Ebene der Richtlinien oder auch generischen Konzepte konkretisiert diese Sicherheits- und Kontinuitätselemente, ist aber systemunabhängig und -übergreifend. Durch die Richtlinien können die Verantwortlichen beispielsweise neu anzuschaffende Systeme dahingehend überprüfen, ob sich auf diesen die geforderten Sicherheitsmerkmale realisieren lassen. Gleichzeitig dienen die plattformübergreifenden Vorgaben zur Vereinheitlichung des Sicherheits- und Kontinuitätsniveaus.

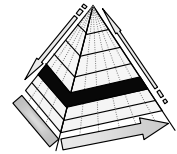
Die Sicherheits- und Kontinuitätsrichtlinien beinhalten prinzipiell Vorgaben zur Prävention, Detektion sowie Meldung und Alarmierung, Reaktion, Restauration und Verifikation. Sie umfassen ferner die PROSim-Elemente Prozesse, Ressourcen und Organisation. Ihre einzelnen Elemente sind in unterschiedlichen Phasen des später beschriebenen Lebenszyklus oder phasenübergreifend relevant.

Sicherheitsrichtlinien, oftmals auch als „policies“ bezeichnet, gibt es u. a. für die IT- und Internet-Nutzung, den Datenschutz, die Datensicherung, den Zutritts-, Zutritts-, Zugangs- und Zugriffsschutz, Firewalls und Computerviren-Schutz, Fernwartung und Outsourcing, Prozesse und Notfallvorsorge sowie den Umgang mit E-Mails, Passwörtern und sensiblen Daten.

Die Sicherheitsrichtlinien schaffen die Basis für die später beschriebenen prozess- oder ressourcenspezifischen Sicherheitskonzepte und -maßnahmen.

Die folgenden Unterkapitel enthalten überblicksartige, prinzipielle und auszugsweise Beispiele für verschiedene Sicherheitsrichtlinien. Diese müssen jeweils unternehmensspezifisch geprüft, angepasst, verändert und ergänzt werden:

1. Übergreifende Richtlinien
2. Begleitprozesse (Managementdisziplinen)
3. Organisation
4. Zusammenfassung



10.1 Übergreifende Richtlinien

Die folgenden Unterkapitel enthalten prinzipielle Beispiele übergreifender Richtlinien und zwar:

1. Sicherheitsregeln
2. Prozessvorlage
3. IT-Benutzerordnung
4. E-Mail-Nutzung

10.1.1 Sicherheitsregeln

Zur generellen Orientierung empfiehlt es sich, Sicherheitsregeln, z. B. in Form von „Geboten“, aufzustellen. Zu diesen Grundregeln des Unternehmens können beispielsweise folgende Elemente gehören:

1. Einhaltung von gesetzlichen und aufsichtsbehördlichen Vorgaben und von Vorschriften sowie Identifizierung und Orientierung an bzw. Einhaltung von sicherheitsrelevanten Standards und Normen
2. Orientierung an den Anforderungen der externen und internen Kunden unter Berücksichtigung der unternehmens- und geschäftsprozessspezifischen Angemessenheit
3. Aufbau und Pflege eines Sicherheits-, Kontinuitäts- und Risikomanagementsystems, orientiert an der Sicherheitspyramide, das hierarchisch aufgebaut ist, Prozesse, Ressourcen und Organisation berücksichtigt sowie in den Lebenszyklus von Prozessen, Ressourcen, Dienstleistungen und Produkten integriert ist
4. Klassifizierung von Geschäftsprozessen, Anwendungen und Daten gemäß ihrer Bedeutung für das Unternehmen und den daraus resultierenden Sicherheitsanforderungen
5. Etablierung eines Grundschutzes sowie darauf aufbauender Sicherheitsklassen
6. Einhaltung des Prinzips des gesperrten Bildschirms
7. Einhaltung des Prinzips des „aufgeräumten“ Arbeitsplatzes
8. Einhaltung des Prinzips des generellen Verbots
9. Einhaltung des Prinzips der minimalen Rechte in allen Sicherheitsbereichen (z. B. Zufahrts-, Zutritts-, Zugangs-, Zugriffsschutz)
10. Einhaltung des Prinzips der minimalen Dienste bei Informations- und Kommunikationssystemen
11. Steuerung des Sicherheits-, Kontinuitäts- und Risikomanagements durch Zielvereinbarungen und deren Controlling

12. Regelmäßige Prüfung des erreichten gegen das geforderte Sicherheits- bzw. Risikoniveau
13. Sicherstellung der Nachvollziehbarkeit, z. B. von Zielen, Vorgaben und sicherheitsrelevanten Aktivitäten und Ereignisse
14. Schulung und Sensibilisierung der Mitarbeiter
15. Festlegung einer Kommunikationsrichtlinie, in der festgehalten ist, wer welche Informationen an Dritte weitergeben darf.

10.1.2 Prozessvorlage

Für die ITK-Betriebs- und Begleitprozesse, die in der Sicherheitsarchitektur angegeben sind, sollte eine angemessene Prozessdokumentation vorhanden sein. Diese enthält die jeweiligen Prozesse mit ihren Prozessschritten und Verbindungsstellen zu anderen Prozessen sowie die Technologien, Methoden, Werkzeuge und Hilfsmittel. Ferner sind hierin die jeweiligen Rollen, die hierfür erforderliche Qualifikation und die Verantwortlichkeiten festgelegt.

ITK-Betriebs- und Begleitprozesse

Hilfsmittel zur Prozessdokumentation sind im einfachsten Fall papiergebunden und handschriftlich, oder sie basieren auf einem Grafikprogramm, selbst entwickelten Tabellen eines Tabellenkalkulationsprogramms oder einer Datenbank. Bei professionellem Einsatz lassen sich am Markt verfügbare Software-Produkte einsetzen.

Hilfsmittel

Um die Lesbarkeit der Prozessdokumentation für die Nutzer zu verbessern, die gewünschte Vollständigkeit zu erreichen und die Effizienz zu steigern, sollte die Prozessdokumentation auf eine einheitliche Weise erfolgen. Es empfiehlt sich, eine standardisierte Gliederungsstruktur vorzugeben. Um den Zugriff für die Beteiligten zu vereinfachen und Aktualisierungen zeitnah zur Verfügung zu stellen, kann eine Portallösung hilfreich sein. Diese sollte auch einen Überblick über die Prozesslandschaft und deren Zusammenspiel geben. Jede einzelne Prozessbeschreibung kann beispielsweise folgendermaßen gegliedert sein:

Standardisierte Prozessdokumentation z. B. als Portal

1. Prozessbezeichnung
2. Prozessnutzer/Adressaten
3. Geltungsbereich
4. Prozessverantwortlicher
5. Prozessziel
6. Prozesskennzahlen
7. Schutzbedarf sowie Sicherheits- und Kontinuitäts- bzw. Risikoklasse

8. Schnittstellen/Verbindungsstellen
9. Prozessablauf
Für jeden Prozessschritt im Prozessablauf werden Input, Schnittstellen, Aktivitäten, Hilfsmittel/ Tools, Richtlinien, Methoden, Verantwortlichkeiten/Rollen, Ergebnistypen sowie deren inhaltliche Struktur festgelegt und beschrieben
10. Qualifikationsprofil je Rolle
11. Prüfungskonzept
12. Testkonzept
13. Schulungskonzept
14. Übungskonzept
15. Pflege- und Weiterentwicklungskonzept
16. Glossar
17. Mitgeltende Dokumente
18. Referenzierte Dokumente

Im Hinblick auf mögliche Prozessschritte sollten weitere Orientierungshilfen gegeben werden. Häufig anzutreffen sind die folgenden Prozessschritte:

- Anforderungen erheben
- Anforderungen transformieren
- Konzepte entwickeln
- Konzepte prüfen
- Konzepte umsetzen
- Prüfungskonzept entwickeln
- Prüfungen durchführen
- Testkonzept entwickeln
- Tests durchführen
- Schulungskonzept entwickeln
- Schulung durchführen
- Umsetzungskonzept entwickeln
- Umsetzung durchführen und überwachen
- Übungskonzept entwickeln
- Übungen durchführen
- Überwachungs- und Übungsergebnisse dokumentieren und analysieren

- Optimierungsvorschläge entwickeln
- Umsetzung verbessern
- regelmäßige Berichte erstellen
- Pflegekonzept entwickeln
- Pflegekonzept umsetzen.

Bei einigen Prozessen sind darüber hinaus folgende Aktivitäten zu definieren:

- gefährliche Ereignisse erkennen
- gefährliche Ereignisse melden, Alarm geben
- (gefährliche) Ereignisse aufzeichnen
- (gefährliche) Ereignisse auswerten
- gefährliche Ereignisse abwehren
- Schaden beurteilen
- Schaden beheben
- regulären Zustand wiederherstellen.

10.1.3 IT-Benutzerordnung

Das folgende Beispiel zeigt eine prinzipielle Benutzerordnung.

IT-Benutzerordnung

Basierend auf der Sicherheits-, Kontinuitäts- und Risikopolitik des <Unternehmens> muss jeder festangestellte und freie Mitarbeiter folgende Regelungen berücksichtigen:

1. Die Prinzipien der „minimalen Rechte“, der „minimalen Dienste“, des „generellen Verbots“, des „gesperrten Bildschirms“ und des „aufgeräumten Arbeitsplatzes“ sind einzuhalten.

Die Prinzipien der „minimalen Rechte“ bzw. der „minimalen Dienste“ besagen, dass Rechte bzw. Dienste stets nur in dem Umfang gewährt werden, wie sie zur Erfüllung der jeweiligen Aufgabenstellung minimal erforderlich sind.

Das Prinzip des „generellen Verbots“ besagt, dass alles verboten ist, was nicht explizit erlaubt ist. Konkret meint dies u. a., dass Rechte und Dienste, sollten sie trotz fehlender Berechtigung nutzbar sein, nicht genutzt werden dürfen.

Die Prinzipien des „gesperrten Bildschirms“ und des „aufgeräumten Arbeitsplatzes“ sagen aus, dass Daten und Informationen am Bildschirm, aber auch Unterlagen und Datenspeicher, wie CDs, mobile Festplatten, USB memory sticks und Notebooks am Arbeitsplatz für Unberechtigte nicht offen zugänglich sein dürfen.



2. Der Benutzer darf nur die Hardware nutzen, z. B. PCs, Notebooks und Memory Sticks, und auch nur in der Ausstattung, in der sie ihm das <Unternehmen> bereitstellt.
3. Der Benutzer darf nur jene Programme (Software) nutzen, die ihm das <Unternehmen> bereitstellt. Eigene Programme oder Programme Dritter dürfen weder eingespielt noch aus dem Internet oder einer anderen Quelle heruntergeladen werden. Sie dürfen darüber hinaus weder installiert noch genutzt werden.
4. Die ITK-Ressourcen, wie z. B. Computersysteme, Telefonanlagen und Telefone, dürfen ausschließlich geschäftlich und nur in dem Umfang genutzt werden, wie es zur Erfüllung der geschäftlichen Aufgaben erforderlich ist. Dies schließt deren Nutzung für außergeschäftliche, z. B. private, nebenberufliche oder rechtswidrige Aktivitäten aus.
5. Es dürfen nur jene ITK-Ressourcen, wie z. B. Computersysteme, Anwendungen und Daten, benutzt werden, für die eine Berechtigung erteilt wurde.
6. Die ITK-Ressourcen, z. B. Computer, Anwendungen und Daten, dürfen nur in dem Umfang genutzt werden, wie es der schriftlich erteilten Berechtigung entspricht.
7. Benutzer dürfen die vom <Unternehmen> bereitgestellte Software weder kopieren noch verändern oder veräußern.
8. Jeder Benutzer muss seine Passwörter vertraulich behandeln. Sie dürfen nur ihm bekannt sein. Eine Weitergabe von Passwörtern ist in keinem Fall zulässig, selbst dann nicht, wenn eine Person vertrauenswürdig und zu deren Kenntnis berechtigt erscheint.
9. Der Benutzer ist für alle Aktivitäten verantwortlich, die unter seiner Benutzerkennung und seinem Passwort durchgeführt werden.
10. Der Benutzer darf keine Benutzerkennungen und Passwörter Dritter benutzen. Dritte können z. B. sowohl „übliche“ Benutzer als auch „technische“ Benutzer sein.
11. ITK-Ressourcen, wie z. B. Computer, Anwendungen, Datenträger und Daten, dürfen nur wenn erforderlich und auch dann ausschließlich von autorisierten Personen an autorisierte Dritte weitergegeben werden.
12. Der Benutzer ist verpflichtet, alle Richtlinien und Regeln des Sicherheits-, Kontinuitäts- und Risikomanagements des <Unternehmens> in ihrer jeweils aktuellen Form einzuhalten. Hierzu gehören insbesondere:
 - Richtlinie Zugangsschutz
 - Richtlinie Zugriffsschutz
 - die Passwortregeln (Ge- und Verbote)
 - Richtlinie Computerviren-Schutz
 - die Richtlinie E-Mail-Nutzung (Ge- und Verbote)
 - die Richtlinie Internet-Nutzung (Ge- und Verbote)

13. Verstöße gegen die IT-Benutzerordnung aufgrund beabsichtigten oder grob fahrlässigen Verhaltens können mit angemessenen Sanktionen belegt werden. Verstöße können z. B. Schadensersatzansprüche sowie straf-, zivil- und arbeitsrechtliche Konsequenzen nach sich ziehen.
14. ...

10.1.4 E-Mail-Nutzung

Das folgende Beispiel zeigt auszugsweise eine prinzipielle E-Mail-Richtlinie.

Richtlinie E-Mail-Nutzung

Allgemeines

1. Die Beantragung, Prüfung, Genehmigung, Einrichtung und Rücknahme von E-Mail-Adressen sowie die Aufbewahrung der Anträge erfolgt nach dem „Antrags- und Genehmigungsverfahren E-Mail“.
2. Die Vergabe von E-Mail-Adressen erfolgt nach der „Namenskonvention E-Mail-Adresse“.
3. Personenbezogene E-Mail-Adressen werden bei Ausscheiden eines Mitarbeiters durch den Bereich Informationsservices entsprechend dem „Antrags- und Genehmigungsverfahren E-Mail“ gelöscht. In Einzelfällen kann für eine Übergangsfrist
 - eine Umleitung zu einem anderen Verantwortlichen oder
 - eine automatische Antwort-E-Mail mit dem Hinweis auf die Ungültigkeit der E-Mail-Adresse genehmigt werden.
 Bei einer Umleitung ist die Einhaltung eventueller datenschutzrechtlicher Bestimmungen zu beachten. Bei einer automatischen Beantwortung sind die Folgen im Falle eingehender Spam-Mails zu berücksichtigen.
 Die Information über das Ausscheiden eines Mitarbeiters erhält der Bereich Informationsservices vom Bereich Personalservices gemäß dem „Antrags- und Genehmigungsverfahren E-Mail“.
4. Die E-Mail-Anwendung ist seitens des Bereichs Informationsservices so einzustellen, dass die Vorschau-Funktion für E-Mails deaktiviert ist, damit eingehende E-Mails nicht automatisch und ohne Zutun des Benutzers geöffnet werden. Andernfalls besteht die potenzielle Gefahr, dass eventuelle schädliche Inhalte einer E-Mail ausgeführt werden.
5. Clients sind seitens des Bereichs Informationsservices so zu konfigurieren, dass sie Bestätigungsanforderungen des Absenders nicht automatisch beantworten.
6. Clients sind seitens des Bereichs Informationsservices so zu konfigurieren, dass bei Anzeige von HTML-formatierten E-Mails keine aktiven Inhalte ausgeführt werden. Dies gilt auch, falls für die Anzeige solcher E-Mails ein Browser zum Einsatz kommt.



7. Als Standardapplikationen unter Windows stellt der Bereich Informationsservices nur solche ein, die keine Makros oder Skripte ausführen können. Für Microsoft®-Word oder Microsoft®-Excel beispielsweise existieren derartige „Viewer“. Für den Dateityp „.reg“ wird ein Editor als Standardapplikation konfiguriert.

8. ...

Gebote

1. Die Konfiguration der Clients darf ausschließlich vom Bereich Informationsservices vorgenommen und geändert werden.
2. Das E-Mail-System und die dienstliche E-Mail-Adresse dürfen nur zu dienstlichen Zwecken genutzt werden.
3. Das definierte Standardformat unserer E-Mails einschließlich Haftungsausschluss (Disclaimer) ist einzuhalten.
4. Jede E-Mail muss einen aussagekräftigen Betreff haben, der den unternehmensspezifisch vorgegebenen Aufbau hat. Im Betreff wird gekennzeichnet, welchen Vertraulichkeitsstatus die E-Mail hat.
5. Vertrauliche Nachrichten sind verschlüsselt zu übermitteln.
6. Die Übermittlung rechtsverbindlicher Informationen per E-Mail muss den Regelungen des Unternehmens entsprechen und entsprechend den Unterschriftenregelungen des Unternehmens mit elektronischer Signatur versehen sein.
7. Der oder die Anhänge eingehender E-Mails dürfen nur geöffnet werden, wenn die jeweilige E-Mail vertrauenswürdig ist. Vertrauenswürdig heißt, dass der Absender bekannt ist und die E-Mail in der Betreffzeile einen erwartbaren Text in der mit dem Kommunikationspartner üblichen Sprache enthält. Anzeichen nicht vertrauenswürdiger E-Mails sind unbekannte Absender oder fehlende Absenderangabe oder unerwartete Betreffzeilen, z. B. sinnlose Aneinanderreihungen von Buchstaben, bekannte Absender mit einem Betreff in einer anderen Sprache als der sonst mit dem Kommunikationspartner üblichen sowie Antworten („Re“ der „AW“) trotz fehlender vorheriger diesbezüglicher Korrespondenz.
8. Anhänge von E-Mails, die ausführbaren Code enthalten und/oder Änderungen in der Systemkonfiguration vornehmen könnten, dürfen nur nach Zustimmung des zuständigen Mitarbeiters aus dem Bereich Informationsservices gestartet werden.
9. ...

Verbote

1. Versendete E-Mails dürfen keinen schädigenden Zweck, z. B. die Verbreitung von Viren oder Massen-E-Mails (Spamming) oder die Blockade von Systemen und Diensten (Denial-of-Service-Attacks (DoS)), verfolgen.

2. Versendete E-Mails dürfen keine Schadsoftware, wie z. B. Viren, enthalten.
3. Versendete E-Mails dürfen keine Kettenbriefe sein.
4. Die Versendung von Massen-E-Mails (Spam) ist verboten.
5. Die E-Mail-Absenderangabe versendeter E-Mails darf nicht verfälscht sein.
6. Versendete E-Mails dürfen keine gesetzwidrigen, anstößigen, belästigenden, beleidigenden, drohenden, Gewalt verherrlichenden, kriminellen, terroristischen, diskriminierenden, rassistischen, sexistischen oder pornographischen Inhalte haben.
7. Versendete E-Mails dürfen keine Inhalte haben, die das Unternehmen oder sein Image schädigen können.
8. Versendete E-Mails dürfen keine unzulässigen Kopien von urheberrechtlich geschützten Werken enthalten.
9. E-Mails dürfen nicht automatisch an Adressen außerhalb des Unternehmens weitergeleitet werden.
10. Private E-Mails sind prinzipiell verboten. Im Einzelfall darf der Nutzer eine private E-Mail versenden, jedoch nur dann, wenn dadurch weder das Unternehmen noch die eigene Arbeitsleistung beeinträchtigt oder gestört werden. Außerdem sollten private E-Mails über den privat genutzten E-Mail-Provider und mit der privaten E-Mail-Adresse versendet werden. Bei Versand einer privaten E-Mail unter der dienstlichen E-Mail-Adresse sind alle unternehmensspezifischen Regelungen zu E-Mails einzuhalten. Außerdem willigt der Nutzer in diesem Fall ein, dass diese E-Mails gespeichert werden und bei Bedarf geprüft werden können.
11. Die dienstliche E-Mail-Adresse darf ausschließlich bekannten und vertrauenswürdigen Geschäftspartnern bekannt gemacht werden.
12. Links eingehender E-Mails dürfen nicht angeklickt werden, sondern müssen geprüft und bei Bedarf manuell im dienstlich bereit gestellten Browser eingegeben werden.
13. Die Beantwortung von Spam-Mails, z. B. zur Löschung aus deren Verteiler, ist verboten, im Gegensatz zur zulässigen Abbestellung nicht mehr benötigter, aber bisher abonnierter Informations-E-Mails.
14. Nachrichten, die rechtsverbindlichen Charakter haben, dürfen ohne Einhaltung der unternehmensspezifischen Regelungen und ohne elektronische Signatur nicht als E-Mail versandt werden, sondern müssen in Papierform mit rechtsverbindlichen Unterschriften entsprechend den Unterschriftenregelungen des Unternehmens übermittelt werden.
15. ...

10.1.5 Internet-Nutzung

Das folgende Beispiel zeigt auszugsweise eine prinzipielle Richtlinie zur Internet-Nutzung.



Richtlinie Internet-Nutzung

Allgemeines

1. Die Berechtigungvergabe zur geschäftlichen Nutzung des Internets erfolgt auf der Basis des Prinzips der „minimalen Dienste“, d. h. der Internetzugang wird nur dann gewährt, wenn dies zur Aufgabenerfüllung minimal erforderlich ist.
2. Die Beantragung, Prüfung, Genehmigung, Einrichtung und Rücknahme des Internet-Zugangs sowie die Aufbewahrung der Anträge erfolgt nach dem „Antrags- und Genehmigungsverfahren Internet-Zugang“.
3. Die Anbindung an das Internet erfolgt stets über einen Firewall.
4. Bei ITK-Ressourcen, wie z. B. Clients und Servern, die an das Internet angebunden sind, stellt der Bereich Informationsservices sicher, dass die Gefährdung für das interne Netz so niedrig ist, dass die Sicherheitsanforderungen aller anderen Ressourcen in diesem Netz eingehalten werden. Dies kann es erforderlich machen, Netzsegmente mit unterschiedlichem Sicherheitsniveau zu schaffen und gegeneinander abzusichern, z. B. in Form von VLANs (virtuelle LANs).
5. ITK-Ressourcen, wie z. B. Server, die Dritten, z. B. Kunden, den Zugang über das Internet, z. B. in Form eines Extranets, ermöglichen, installiert der Bereich Informationsservices in einer demilitarisierten Zone. Dadurch ist diese ITK-Ressource sowohl gegenüber dem Internet durch einen Firewall als auch das interne Netz gegenüber der ITK-Ressource durch einen Firewall geschützt. So lässt sich das interne Netz vor der Bedrohung durch eine eventuelle Kompromittierung der ITK-Ressource infolge eines Hacker-Angriffs schützen.
Die Kommunikation zu ITK-Ressourcen im Extranet vom internen Netz aus wird ausschließlich vom internen Netz her aufgebaut. Dadurch lassen sich Kommunikationsversuche durch derartige ITK-Ressourcen, z. B. infolge einer Kompromittierung, sperren und eine Meldung auslösen.
6. ...

Gebote

1. Das Internet darf nur zu dienstlichen Zwecken und im Rahmen der eigenen dienstlichen Aufgaben genutzt werden.
2. ...

Verbote

1. Es dürfen keine Internet-Seiten mit gesetzwidrigen, beleidigenden, drohenden, gewaltverherrlichenden, kriminellen, terroristischen, rassistischen, sexistischen oder pornographischen Inhalten besucht werden.
2. Es dürfen keine Anwendungen aus dem Internet heruntergeladen werden.
3. Eine Teilnahme an webbasierten Umfragen ist verboten.
4. ...

10.2 Betriebs- und Begleitprozesse (Managementdisziplinen)

Für die verschiedenen Betriebs- und Begleitprozesse (Managementdisziplinen), die in der Sicherheitsarchitektur angegeben wurden, ist zu prüfen, ob plattformunabhängige Richtlinien angemessen sind. In den folgenden Unterkapiteln sind unter dem Fokus Betriebs- und Angriffssicherheit sowie Kontinuität auszugswise prinzipielle Beispiele derartiger Richtlinien angegeben, die an die jeweiligen Gegebenheiten angepasst werden müssen.

Der Vollständigkeit halber sei erwähnt, dass es sich empfiehlt, für alle in der Sicherheitsarchitektur genannten Prozesse Sicherheitsrichtlinien aufzustellen, wenngleich im Folgenden aus Platzgründen nur für einige der zuvor genannten Begleitprozesse Beispiele aufgenommen worden sind. Außerdem sollten sich die Richtlinien am Lebenszyklus von IT-Systemen orientieren, wie ihn der Autor in einem späteren Kapitel beschrieben hat. Beispiele für lebenszyklusorientierte Richtlinien finden Sie verschiedentlich in den folgenden Unterkapiteln.

10.2.1 Kapazitätsmanagement

Die folgende Richtlinie gibt ein prinzipielles Beispiel einer Richtlinie für das Kapazitätsmanagement.

Richtlinie Kapazitätsmanagement

Allgemeine und phasenübergreifende Vorgaben

1. Die Planung, Erhebung, Dokumentation, Umsetzung, Überwachung und regelmäßige Aktualisierung der aktuellen und zukünftigen Anforderungen an Kapazität und Performance integriert der Bereich Informationsservices in den Lebenszyklus von Prozessen und Ressour-



cen.
2. ...
Planungsphase
1. Die aktuellen und zukünftigen Anforderungen an Kapazität und Performance erhebt der Bereich Informationsservices in der Planungsphase. Er dokumentiert und berücksichtigt sie.
2. ...
Fachkonzeptionsphase
1. Der Auftraggeber bzw. der auftraggebende Fachbereich konkretisiert und verifiziert die erhobenen fachlichen Anforderungen an Kapazität und Performance in der Konzeptionsphase.
2. Der Auftraggeber bzw. auftraggebende Fachbereich legt die fachlichen Messkriterien und deren Zielwerte sowie als Prozentzahlen deren Grenzwerte für Warnung und Alarmierung fest.
3. Der Auftraggeber bzw. auftraggebende Fachbereich spezifiziert die Anforderungen an das Monitoring und Reporting aus fachlicher Sicht.
4. ...
Technische Konzeptionsphase (Grob- und Feinkonzept)
1. Der Bereich Informationsservices berücksichtigt die erhobenen Anforderungen an Kapazität und Performance in den technischen Konzepten.
2. Der Bereich Informationsservices transformiert die fachlichen Anforderungen auf technische Ressourcen. Für jede Ressource spezifiziert er die technische Realisierung zur Erfassung und Überwachung der Messkriterien einschließlich Warnung und Alarmierung sowie einzusetzender Tools.
3. Der Bereich Informationsservices leitet aus den fachlichen Anforderungen die Inhalte und die Häufigkeit der technischen Berichte ab. In monatlichen Berichten sind üblicherweise Informationen zur Kapazität und Performance der verschiedenen Ressourcen im Hinblick auf Plan, Ist und Prognose absolut und prozentual sowie im Durchschnitt anzugeben. Ferner werden die Spitzenwerte und deren Häufigkeit angeführt.
4. ...
Entwicklungsphase
1. Der Bereich Informationsservices realisiert die erhobenen Anforderungen an Kapazität und Performance während der Entwicklung.
2. ...

Testphase

(Integrations- und Systemtest einschließlich Freigabe und Abnahme)

1. Der Bereich Informationsservices sowie die Fachbereiche testen durch geeignete Szenarien die Erfüllung der Kapazitäts- und Performanceanforderungen sowie der Berichte aus fachlicher bzw. technischer Sicht unter Berücksichtigung der Sicherheitsklasse in angemessenem Umfang.
2. ...

Inbetriebnahme- und Betriebsphase

1. Der Bereich Informationsservices überwacht (monitoring) die Kapazität und Performance kontinuierlich. Er analysiert Abweichungen und nimmt Optimierungen vor, z. B. Tuning von Datenbanken.
2. Der Bereich Informationsservices aktualisiert die aktuellen und zukünftigen Anforderungen an die Kapazität und Performance der verschiedenen Ressourcen regelmäßig.
3. Der Bereich Informationsservices beobachtet technologische Entwicklungen und neue Erkenntnisse, schätzt ihren Nutzen ab und ergreift gegebenenfalls daraus abgeleitete Maßnahmen.
4. Der Bereich Informationsservices sowie die Fachbereiche werten die verschiedenen Berichte aus und ergreifen bei Bedarf Optimierungsmaßnahmen, z. B. Einsatz leistungsfähigerer Prozessoren, Speicher- oder Druckeinheiten sowie Netzkomponenten.
5. ...

Außerbetriebnahmephase

1. Die Außerbetriebnahme eines Systems oder einer Anwendung schließt die Überprüfung der eventuell erforderlichen Außerbetriebnahme jener Tools und die Beendigung oder Reduzierung jener Lizenzverträge ein, die zur Kapazitäts- und Performance-Messung eingesetzt wurden.
2. ...

10.2.2 Kontinuitätsmanagement

Für das Kontinuitätsmanagement sind Richtlinien für die folgenden Themenkomplexe zu definieren:

- Vermeidung durch Prävention
- Datensicherung einschließlich deren Umfang, Zeitpunkt, Aufbewahrung und Auslagerung
- Notfall- und Katastrophenvorsorgeplanung einschließlich Wiederanlaufverfahren.

10.2.2.1 Vermeidung durch Prävention

Die folgende Tabelle zeigt ein auszugsweises und prinzipielles Beispiel einer überblicksartigen Richtlinie für unterschiedliche sicherheitsrelevante Räumlichkeiten. Die konkreten Räumlichkeiten in der Tabelle, z. B. Rechenzentrum, lassen sich durch entsprechende Schutzbedarfsklassen ersetzen und verallgemeinern.

Sicherheitselement	RZ	SR	TR	DR
Allgemeines				
Einhaltung von Normen und Vorschriften, z. B. DIN, VDE, VdS	Z	Z	Z	Z
jederzeit aktuelle Pläne der Räumlichkeiten und ihrer Ausstattung einschließlich Plänen der Leitungsführung und gegebenenfalls Verrohrung	Z	Z	Z	Z
Doppelboden ausreichender Höhe und Tragfähigkeit	Z	B	B	B
ausreichend dimensionierte Kabeltrassen	Z	Z	Z	Z
geschützte Kabelführung	Z	Z	Z	Z
Trennung von Telekommunikations- und Stromleitungen	Z	Z	Z	Z
eindeutige Kennzeichnung der Kabel	Z	Z	Z	Z
regelmäßige fachgerechte Wartung von Systemen und Anlagen durch qualifiziertes Personal gemäß empfohlenen Wartungsintervallen und unter Berücksichtigung eventueller versicherungstechnischer Anforderungen sowie Dokumentation der Durchführung in Wartungsprotokollen	Z	Z	Z	Z
Regelmäßige fachgerechte Wartung von Systemen und Anlagen gemäß Vorgaben sowie Wartungsdokumentation	Z	Z	Z	Z
Aufschaltung von Meldeeinrichtungen auf einen rund um die Uhr besetzten Leitstand	Z	Z	Z	Z
...				
Zutrittsschutz				
Richtlinie Zutrittsschutz	Z	Z	Z	Z
Zutrittskontrolle	Z	Z	Z	Z
Vereinzelungsanlage	Z	B	B	B
Videoüberwachung und -aufzeichnung	Z	B	B	B
...				

Sicherheitselement	RZ	SR	TR	DR
<u>Klimatisierung</u>				
Wärmelastberechnung, deren Pflege und Umsetzung	Z	Z	Z	B
Klimaanlage	Z	Z	B	Z
Klimaüberwachung und Alarmierung	Z	B	B	Z
...				
<u>Brandschutz</u>				
Rauchverbot	Z	Z	Z	Z
Handfeuerlöscher	Z	Z	Z	Z
Brandmeldeanlage	Z	Z	Z	Z
Brandfrühesterkennung	Z	B	B	B
eigener Brandabschnitt	Z	Z	B	Z
Brandschutztüren und -fenster	Z	B	B	B
Brandschottung von Durchbrüchen	Z	Z	B	Z
Brandlastreduzierung	Z	Z	Z	Z
geeignete Löscheinrichtungen	Z	B	B	B
Sauerstoffreduzierung	B	B	B	B
...				
<u>Einbruchsschutz</u>				
Einbruchmeldeanlage	B	B	B	B
Türen geeigneter Widerstandsklasse	Z	Z	Z	Z
Vermeidung von Fenstern; alternativ: geschützte Fenster geeigneter Widerstandsklasse	Z	Z	Z	Z
Vermeidung von Decken-/Dachfenstern oder -luken	Z	Z	B	Z
...				
<u>Flüssigkeitsschutz</u>				
Vermeidung flüssigkeitsführender Anlagen und Rohre im, über und neben den Räumlichkeiten, z. B. Klimaanlage, Sanitäreinrichtungen	Z	Z	B	Z
Vermeidung von Decken-/Dachfenstern oder -luken	Z	Z	B	Z
Wassermeldeanlage	Z	B	B	B
...				

Sicherheitselement	RZ	SR	TR	DR
<u>Stromversorgung</u>				
Verbrauchsberechnung, deren Pflege und Umsetzung	Z	Z	Z	B
Unterbrechungsfreie Stromversorgung (Voltage and Frequency Independent (VFI), vergleichbar mit der Online-USV mit Dauerwandler)	Z	Z	B	B
Netzersatzanlage (Notstromversorgung)	Z	B	B	B
Redundante Stromversorgungsanbindung	Z	B	B	B
Redundante Leitungsführung für Strom				
- inhouse	Z	Z	B	B
- extern	Z	B	B	B
Überspannungsschutz, bestehend aus Grob-, Mittel- und Feinschutz	Z	Z	Z	B
leicht erreichbarer Not-Aus-Schalter mit Schutz vor unbeabsichtigtem Auslösen	Z	B	B	B
...				
<u>Kommunikation</u>				
Patch-Feld mit Patch-Liste der hergestellten Verbindungen	Z	B	B	B
Redundante Kommunikationsanbindung	Z	B	B	B
Redundante Leitungsführung für Kommunikation	Z	B	B	B
- inhouse	Z	Z	B	B
- extern	Z	B	B	B
...				
Legende: Z = zwingend, B = bei Bedarf, RZ = Rechenzentrum, SR = Serverraum, TR = Technikraum, DR = Datenträgerraum				



Entfernung
zwischen
redundanten
Räumlichkeiten

Entfernung zwischen redundanten Räumlichkeiten

Im Zusammenhang mit Präventionsmaßnahmen wurde ich des Öfteren gefragt, welche Entfernung bzw. welcher Abstand zwischen redundanten Räumlichkeiten liegen sollte. Die Antwort hierauf ist zuallererst abhängig von den gestellten Sicherheitsanforderungen und den Rahmenbedingungen.

Für denjenigen, der nur die Bedrohung durch Feuer absichern will, kann bei Technikräumen die Nutzung separater Brandabschnitte ausreichend sein. Wer andererseits die RAID-Definitionen beispielsweise auf Räumlich-

keiten anwendet, erhält für den Level DTDS für Katastrophentoleranz eine Entfernung von 1 km, für den Level DTDS+, eine Entfernung von 10 km.

Das deutsche BSI hat sich in einer datumsfreien Unterlage [76], die nach dem Stromausfall im Münsterland, der sich im November 2005 ereignete, entstanden ist, zum Thema Entfernung geäußert und zwar bei Rechenzentren. Das BSI führt hierin bei seinen Grundüberlegungen aus, dass RZs so liegen sollten, „dass sie möglichst nicht gleichzeitig durch das gleiche Schadensereignis betroffen sein können“. Diese Formulierung ähnelt dem Müllerschen Distanzprinzip aus dem „Handbuch Unternehmenssicherheit“, das im Oktober 2005 erschienen ist, wenngleich es nur einen Teil davon anspricht.

Unter Berücksichtigung eines Sperr-Radius von 1,5 km um einen Standort bei realistischen Bedrohungsszenarien nennt das BSI-Dokument einen Minimalabstand von 5 km. Den Maximalabstand bestimmen demzufolge „meist übertragungstechnische Aspekte“, die „typischerweise ab ca. 10 bis 15 km“ beginnen. Das BSI sieht kaum realistische Schadensereignisse, die bei einer solchen Entfernung beide RZs gleichzeitig nicht mehr betreibbar machen.

Eine aus Sicht des Autors recht geeignete Formulierung lässt sich aus [77], Section 4030.1, S. 1, „Alternate Operating Headquarters“ sowie aus „Sound Practices for the Management and Supervision of Operational Risk“ [34] ableiten und verallgemeinern. Die Müllersche Distanzanforderung bzw. das Müllersche Distanzprinzip des Autors, veröffentlicht im „Handbuch Unternehmenssicherheit“, lautet folgendermaßen:

Ausweichprozesse und -ressourcen, z. B. Gebäude und Räume, sollten soweit vom Originalstandort entfernt liegen, dass sie nicht während des gleichen Zeitraums von solchen gleichen oder miteinander zusammenhängenden Bedrohungen betroffen sind, die abgesichert werden sollen.

10.2.2.2 Datensicherungsrichtlinie

Das folgende prinzipielle Beispiel enthält Elemente einer Datensicherungsrichtlinie.

Richtlinie Datensicherung

Allgemeine und phasenübergreifende Vorgaben

1. Die Datenträger müssen jederzeit eindeutig identifizierbar sein. Daher ist die hierfür definierte „Namenskonvention Datensicherungsträger“ einzuhalten.
2. Die Inhalte der Datensicherungsträger und deren Quelle müssen ebenso wie der/die einer Quelle zugeordnete(n) Datensicherungsträger jederzeit kurzfristig ermittelbar sein.



3. Das zur Datensicherung eingesetzte Tool und die gewählte Parametrierung muss nachvollziehbar sein.
4. Das Verfahren zur Rekonstruktion der Daten muss beschrieben sein.
5. Programm- und Konfigurationsdaten sind zumindest nach jeder Änderung zu sichern. Hierzu gehören ebenfalls Änderungen von Einheitentreibern etc.
6. Anwenderdaten sind – orientiert an den Anforderungen – regelmäßig zu sichern, üblicherweise arbeitstäglich.
7. Die Daten sind – abhängig vom Schutzbedarf – auf den Datenträgern verschlüsselt zu speichern. Ein geeignetes und sicheres Schlüsselmanagement ist zu etablieren und dessen jederzeitige Verfügbarkeit sicherzustellen.
8. Die Korrektheit jeder Datensicherung ist sicherzustellen, z. B. durch Überprüfung.
9. Bei der Datensicherung ist das Generationenprinzip zu berücksichtigen, üblicherweise das Urgroßvater-Großvater-Vater-Sohn-Wechselschema. Die verschiedenen Mediasets sind ihrer Generationenzugehörigkeit entsprechend zu beschriften, wie in der „Namenskonvention Datensicherungsträger“ festgelegt.
10. Die Art der Datensicherung, d. h. vollständig, inkrementell, differenziell oder selektiv, ist festzulegen. Hierbei sind die erhobenen Anforderungen, das aktuelle und das prognostizierte Sicherungsvolumen, das Sicherungsfenster und die Rückspeicherungsdauer zu berücksichtigen.
11. Die Medien zur Datensicherung (z. B. Datenband, Festplatte) sind unter Berücksichtigung der Anforderungen festzulegen.
12. Die Nutzungsdauer von Sicherungsmedien muss auf ihre Lebenserwartung ausgerichtet sein. Sicherungsmedien werden daher mit dem Datum der Anschaffung und Erstsicherung sowie der Aussonderung versehen, um alterungsbedingten Effekten durch präventiven Ersatz entgegenwirken zu können.
13. Die Aussonderungsfristen der Datenträger sind zu überwachen.
14. Sicherungsmedien, die ausgesondert werden, sind vertraulich zu vernichten.
15. Die Anforderungen sowie die Eckdaten zur Datensicherung sind in einer zugriffsgeschützten und replizierten Datenbank zu speichern. Diese kann über das Intranet angesprochen werden.
16. Datensicherungen sind Zutritts geschützt an einem geeigneten Ort aufzubewahren. Abhängig von den Sicherheitsanforderungen muss mindestens bei älteren Sicherungsgenerationen zusätzlich eine hinreichende räumliche Trennung vorhanden sein. Der Aufbewahrungsort muss geeignete Umfeldbedingungen, z. B. hinsichtlich Temperatur und Luftfeuchtigkeit bereitstellen, sowie Schutz vor Magnetismus, Feuchtigkeit, Brand, Rauch, Staub, korrosiven Gasen, Diebstahl etc.

bieten. Dies können z. B. spezielle Daten-Safes sein.

17. Die Zutrittsberechtigungen zum Sicherungsarchiv sind zu dokumentieren.
18. Der Zutritt zum Sicherungsarchiv ist zu protokollieren.
19. Veränderungen im Sicherungsbestand (Zu-, Abgänge, Austausch) sind zu protokollieren.
20. Die Datensicherungspläne sind mindestens einmal pro Jahr auf Gültigkeit und Inhalt zu überprüfen.
21. Die Datensicherungsverfahren sind mindestens einmal jährlich im Hinblick auf technologische Veränderungen zu überprüfen.
22. Wenn es unter Kosten-Nutzen-Aspekten sinnvoll erscheint, sollte ein Datenträgerverwaltungssystem zum Einsatz kommen, welches das Datenträgerkataster führt, Onlineabfragen gestattet und die Aussonderungsfristen überwacht. Die Informationen über Datenträger sowie deren Inhalte sind abzusichern.
23. ...

Fachkonzeptionsphase

1. Die Anforderungen an die Datensicherung sind im Rahmen der Schutzbedarfsanalyse zu erheben.
2. ...

Technische Konzeptionsphase (Grob- und Feinkonzept)

1. Die Verantwortlichkeit sowie das Vorgehen für die Datensicherung sind einschließlich der Stellvertreterregelung gemäß der Dokumentationsvorlage zur Datensicherung zu dokumentieren.
2. ...

Testphase

(Integrations- und Systemtest einschließlich Freigabe und Abnahme)

1. Der Bereich Informationsservices testet unter bedarfsorientierter Einbindung des Fachbereichs die vollständige Dokumentation sowie die Funktionsfähigkeit des Datensicherungsverfahrens unter Berücksichtigung fachlicher, funktionaler, technischer und zeitlicher Aspekte von der Datensicherung über die Lesbarkeit der Datensicherungsträger und die Auslagerung bis hin zum Rückspielen der Daten. Der Fachbereich prüft die zurückgespielten Daten auf Korrektheit und Nutzbarkeit.
2. ...

Inbetriebnahme- und Betriebsphase

1. Im Betrieb protokolliert der Bereich Informationsservices die durchgeführten Datensicherungen, deren Lesbarkeitsprüfung und Auslagerung.
2. Der Bereich Informationsservices stellt die Einhaltung der allgemeinen

und phasenübergreifende Vorgaben sicher. Hierzu überprüft er regelmäßig die erstellten Protokolle und Meldungen sowie die Einhaltung der Verfahren.

3. ...

Außerbetriebnahmephase

1. Vor der Außerbetriebnahme verifiziert der Bereich Informationsservices mit dem Fachbereich, dass die Datensicherungen endgültig vernichtet werden dürfen.

2. ...

10.2.2.3 Notfall- und Katastrophenvorsorge

Für die Notfall- und Katastrophenvorsorge sollten entsprechende Handbücher erstellt werden. Zur Steigerung der Effizienz und Vollständigkeit sollte auch hier eine Gliederungsstruktur vorgegeben werden. Diese kann sich z. B. an die Gliederungsstruktur in [70] anlehnen. Die folgende Gliederungsstruktur orientiert sich in deutlich abgewandelter und ergänzter Form hieran:

1. Deckblätter (Dokumententitel, Version, Status, Speicherdatum, Gültigkeitsvermerk, Vertraulichkeitsstufe, Herausgeber, Autor, Ansprechpartner, Änderungsliste, Freigabevermerk, Verteiler)
2. Inhaltsverzeichnis
3. Zielsetzung
4. Geltungsbereich (Standorte, Bereiche, Prozesse)
5. Zielgruppe(n)
6. Definition, z. B. Störung, Notfall, Katastrophenfall
7. Rechtliche Aspekte und Ausführungsbestimmungen
8. Ausfallfolgen und abgeleiteter Planungsumfang
9. Eskalationspfad (Alarmierungsplan {call tree}: z. B. Mitarbeiter/Technik → Leitwarte/-stand {control centre} → Sicherheitsbeauftragter → Krisenmanager → Krisenstab)
10. Mitarbeiter
(Hausnotruf, Meldungsschema, Handlungsanweisungen für spezielle Auslöser {z. B. Unfall, Krankheit, Brand, Verrauchung, Wassereinbruch, Demonstration, Streik, Bombendrohung, Räumung, Geiselnahme, Sabotage, Explosion, Einbruch, Diebstahl, Vandalismus, Erdbeben, Ausfälle von Versorgungseinrichtungen, Räumlichkeiten, Gebäuden, Haustechnik, ITK oder Personal})
11. Leitwarte/-stand (control centre)
12. User Help Desk

13. Krisenstab

(Krisenstab {Mitglieder einschließlich Krisenmanager, Einberufung, Treffpunkt(e), Ausstattung des Krisenzentrums, u. a. mit Arbeitsplätzen, Telefonen, PCs/Notebooks, BCM-Handbuch/-Tool (Papier, CD, USB-Stick) und Drucker, Aufgaben, beteiligte Organisationseinheiten, Rollen und deren Aufgaben, Verantwortlichkeiten und Kompetenzen}, Krisenteams, z.B. zur Bewertung des Schadens (Schadensbewertungsteam) und zur Bewertung der Auswirkungen (Impact Assessment Team), Ablauf im Not-/Katastrophenfall (Checklisten-unterstützt), Bewertungsraster zur Einstufung des Notfalls/der Katastrophe)

14. Prozessbeschreibungen (je Organisationseinheit)

(Prozessname, regulärer Ablauf mit Schnittstellen zu vor- und nachgelagerten sowie unterstützenden Prozessen und Ressourcen, Klassifizierungen, Kennzahlen, Infrastruktur/Arbeitsplätze, Hilfsmittel, Informationssysteme, Tools, Verträge, Versicherungen, Organisation und Personal, szenarienbezogener Übergang (Recovery) zum und Ablauf im Notbetrieb mit Kennzahlen, Infrastruktur/Arbeitsplätzen, Hilfsmitteln, Informationssystemen, Tools, Verträgen, Versicherungen, Notfalllizenzen, Organisation und Personal, Wiederherstellungsprozess sowie Rückkehr in den regulären Betrieb (Recovery) mit Nachbearbeitungsprozess)

15. Berichtswesen (termin- und ereignisgesteuert) mit Verantwortlichkeiten und Inhalten

16. Review- und Testprozess mit Verantwortlichkeiten und entsprechenden Checklisten und Hilfsmitteln, z. B. Testportfolio, -plan, -fall, -sequenz und -protokoll (s. a. die in [78] überblicksartig skizzierte und vom Autor entwickelte Beratungsleistung)

17. Schulungsprozess, -konzept und -unterlagen

18. Übungs- und Verbesserungsprozess mit Verantwortlichkeiten und entsprechenden Checklisten und Hilfsmitteln (s. a. die in [78] überblicksartig skizzierte und vom Autor entwickelte Beratungsleistung), u. a. Übungsportfolio, -plan, -fall, -sequenz, -protokoll und Informationen zu Übungszielen, -bereichen, -arten/-methoden, -objekten, -intervallen, -phasen und -risiken, Rahmenbedingungen (kritische Termine, kritische Zeiträume), Beteiligten, Ergebnisdokumentation und Auswertung

19. Erhebungs-, Aktualisierungs- und Pflegeprozess mit Verantwortlichkeiten für das Notfall- und Katastrophenvorsorge- bzw. BCM-Handbuch/-Portal und die Anlagen, wie z. B. Gebäudepläne, Arbeitsplatzausstattungen

20. Verzeichnis interner und externer Ansprechpartner
(Pförtner, Leitwarte, Betriebsschutz, Betriebsarzt, Sanitäter, Brandschutzhelfer, Haustechnik {Strom, Sanitär, Gas, Telekommunikation}, IT-Services, Versorgungsunternehmen (Strom, Wasser, Gas, Telekommunikation), Externe Hilfsorgane (Polizei, Feuerwehr, Technisches Hilfswerk, Notarzt, Rettungsdienste), Externe Dienstleister {Outsourcer, Sanierung}, Hersteller- und Lieferantenverzeichnis, Versicherer
21. Glossar
22. Abkürzungen
23. Stichwortverzeichnis
24. Mitgeltende Dokumente
25. Referenzierte Dokumente
26. Formulare und Checklisten
27. Anlagen (Gebäudepläne, Arbeitsplatzausstattungen, Hilfsorgane, Hilfseinrichtungen etc.)

*Notfall- und
Katastrophen-
vorsorge-
datenbank*

Erforderliche Informationen lassen sich über ein Notfallplanungstool, ein Textverarbeitungsprogramm, oder eine selbst entwickelte Datenbank erfassen und ablegen. Die Datenbank kann u. a. die Informationen zu den Prozessen, ihrer Kritikalität und den Prozessschritten sowie den dazugehörigen Schutzobjekten, wie z. B. Gebäuden, Räumlichkeiten, Arbeitsmitteln, Arbeitsplatzausstattungen, Services, Personen, Anwendungen und den genutzten Datenbanken, Betriebssystemen und Rechnern enthalten.

Die Datenbank enthält somit den – wie der Autor es nennt – Interdependenzplan [79] bzw. den Interdependenzbaum oder das Interdependenznetz aus Prozessen und Ressourcen. Bei Ausfall, Verlust oder Beeinträchtigung eines Informationssystems oder einer Komponente lässt sich ein Report ziehen, der angibt, welche Auswirkungen sich hieraus ergeben. Bei Ausfall eines Anwendungssystems können so die betroffenen Prozessschritte bzw. Prozesse herausgefunden werden. Über geeignete Matrizen lässt sich dies auch von Hand über Ausdrucke oder ein Tabellenkalkulationsprogramm ermitteln.

*Notfall-
planungstools*

Zu Beginn der Notfall- und Katastrophenvorsorgeplanung ist festzulegen, welches/welche Tools (Textverarbeitung, Tabellenkalkulation, Datenbank, spezifisches Notfallplanungstool) zum Einsatz kommen sollen. Hierzu ist gegebenenfalls eine übergreifende Produkt- und Herstellerbewertung (Produktevaluation) erforderlich, in der die möglichen Tools ermittelt, analysiert und bewertet werden, um anschließend eine Entscheidung treffen zu können.

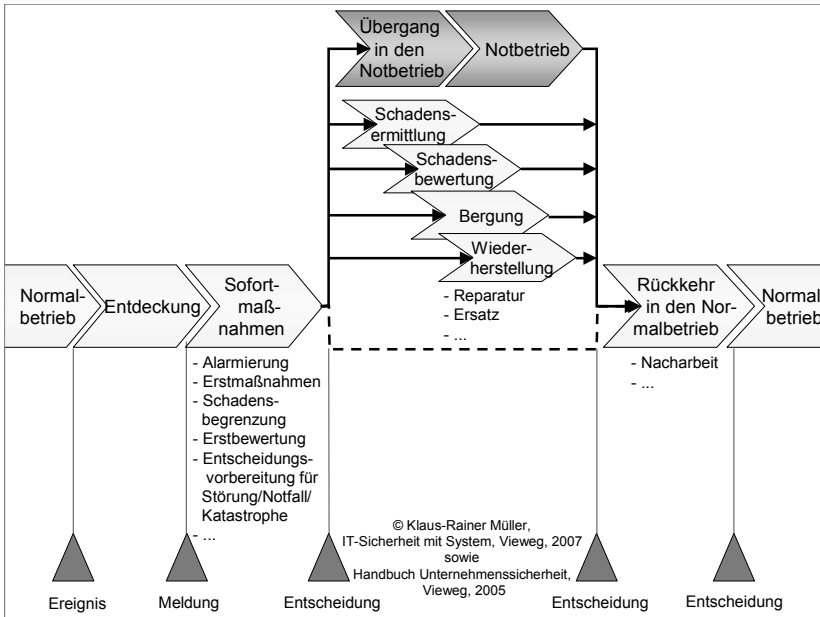


Abb. 10.1: Notfallablauf

In einem Notfall oder einer Katastrophe laufen folgende prinzipielle Phasen ab:

- Ereigniserkennung mit anschließender Meldung
- Sofortmaßnahmen mit Alarmierung, Erstmaßnahmen, Schadensbegrenzung, Erstbewertung, Entscheidungsvorbereitung für das Ausrufen des Notfalls bzw. der Katastrophe
 - Entscheidung über den Verbleib im oder die Rückkehr in den regulären Betrieb oder
 - Entscheidung für Notfall oder Katastrophe:
 - Übergang in den Notbetrieb mit Anlauf der Ersatzobjekte
 - Notbetrieb
 - Schadensermittlung
 - Schadensbewertung
 - Bergung
 - Wiederherstellung bzw. Schadensbehebung
 - Entscheidung für Rückkehr in den regulären Betrieb mit Wiederanlauf und Nacharbeit
- Beendigung des Notfalls/der Katastrophe/des nicht regulären Betriebs.

Recovery- Verfahren

Ein Teil der Notfallplanung befasst sich mit dem Wiederanlauf, d. h. dem Recovery-Verfahren. Da in der Regel für verschiedene Informationssysteme eines Unternehmens Recovery-Verfahren beschrieben sein müssen, empfiehlt es sich, eine standardisierte Gliederungsstruktur vorzugeben. Worauf ist hierbei zu achten?

Zuerst sollten Sie die Anforderungen bzw. Eigenschaften, die das Recovery-Verfahren erfüllen soll, festlegen. Hierzu gehören u. a. die Durchführbarkeit, Korrektheit, Vollständigkeit, Verständlichkeit, Abgestimmtheit, Robustheit, Nachvollziehbarkeit, Know-how-Sicherung, Modularität und Wirtschaftlichkeit.

Im nächsten Schritt legen Sie die Gliederungsstruktur und den Ablauf des Recovery-Verfahrens fest. Dieses reicht von der Ermittlung der Servicevereinbarungen über den Aufbau und Wiederanlauf der Ersatzressourcen bis hin zum Test und der Meldung „ready to go“. Für die Durchführung des Recovery-Verfahrens empfiehlt sich der Einsatz einer Checkliste.

Weitere Verfahren

Weiterhin sind Verfahren für die Prüfung, den Test, die Schulung, Übung und Pflege sowie die Protokollierung festzulegen.



Business Continuity Management Notfall- und Katastrophenvorsorgeplanung

In meiner bisherigen Beratungstätigkeit hat sich des öfteren herausgestellt, dass die Notfall- und Katastrophenvorsorgeplanung bzw. das übergeordnete Business Continuity Management lückenhaft und nicht zielgerichtet waren. Die bisherigen Ausführungen helfen Ihnen, Fehler zu vermeiden. Dennoch empfehle ich Ihnen, zumindest zu Beginn der Konzeptionsphase und mit Ende eines derartigen Projekts sowie für Übungen erfahrene externe Beratung zur Begleitung und Prüfung bzw. zur Qualitätssicherung in Anspruch zu nehmen, um zügig und zielgerichtet voranzukommen.

10.2.2.4 Berichtswesen

Wesentliches Element für die zielgerichtete Steuerung der Verfügbarkeit und Kontinuität der ITK ist ein angemessenes Berichtswesen. Dieses soll u. a. folgende Frage beantworten:

**Welches System bzw. welche Ressource
fällt wie oft wie lange und mit welcher Auswirkung aus?**

Die folgende auszugsweise Richtlinie dient als prinzipielles Beispiel für das Berichtswesen zum Kontinuitätsmanagement

Richtlinie Berichtswesen Kontinuitätsmanagement

1. Prozesse und Ressourcen werden klassifiziert und entsprechend ihrer Sicherheitsklasse im Hinblick auf ihre Verfügbarkeit kontinuierlich überwacht.
2. Für Prozesse und Ressourcen werden Kennzahlen festgelegt, deren Genauigkeit angegeben sowie Zielwerte und Grenzwerte für Warnung und Alarmierung sowie die Messpunkte und das Messverfahren bestimmt.
3. Für die Verfügbarkeit werden Plan-, Ist- und Prognosewerte absolut und prozentual im Durchschnitt und als Spitzenwerte angegeben.
4. Für die Verfügbarkeit werden Ausfallzeiten, -häufigkeit und -folgen im Vergleich Plan zu Ist, absolut und prozentual angegeben.
5. In monatlichen Berichten werden die Plan-, Ist- und Prognosewerte einander gegenübergestellt, analysiert und gegebenenfalls eingeleitete oder empfohlene Maßnahmen beschrieben.
6. ...



10.2.3 Securitymanagement

10.2.3.1 Antrags- und Genehmigungsverfahren

Der Zugang zu den ITK-Systemen muss in schriftlicher Form beantragt werden. Im Hinblick auf die Bearbeitungsgeschwindigkeit und die Wirtschaftlichkeit vorteilhaft ist ein abgesichertes elektronisches Formular, das per Workflow weitergeleitet wird. Alternativ kann ein solches System auch über eine Datenbank abgebildet werden, die über geeignete Zugriffsmechanismen verfügt.

Im elektronischen Formular sind die vom Antragsteller auszufüllenden Felder vorgegeben. Für diese Felder existieren Vorbelegungen, die ausgewählt werden können, z. B. per Listboxen, Combo-Boxen, Checkboxen, ... Zu den – zumindest teilweise – vorbelegbaren Eingabefeldern gehört z. B.:

Antragsteller

- Name und Vorname des Antragstellers
- Personalnummer des Antragstellers bei internen Mitarbeitern, bei externen Mitarbeitern die spezielle externe Mitarbeiternummer
- Organisationseinheit des Antragstellers bzw. Firma und Firmenanschrift bei externen Mitarbeitern
- Funktion des Antragstellers
- Rolle(n) des Antragstellers, z. B. Betriebsrat, Projektmitarbeiter.

<i>Genehmigungs- instanz</i>	Das so ausgefüllte Formular erhält automatisch Datum und Uhrzeit sowie die Signatur des Antragstellers. In einem Workflow-System wird das Antragsformular an die Genehmigungsinstanz(en), z. B. den Leiter der zuständigen Organisationseinheit, weitergeleitet. Er oder die zuständige Instanz genehmigt den Antrag.
<i>Vergabeinstanz</i>	Nach der Genehmigung gelangt der Antrag zur Vergabeinstanz, der Benutzeradministration. Sie prüft den Antrag auf Vollständigkeit, Konsistenz und Korrektheit. Im Falle eines elektronischen Antragsformulars kann diese Prüfung bei geeigneter Auslegung der Eingabemasken weitestgehend entfallen. Außerdem ist eine zumindest überwiegend automatische Einrichtung des Benutzers und seiner Berechtigungen durch das System möglich. Die endgültige Freigabe sollte im Sinne des „Vier-Augen-Prinzips“ jedoch durch den Benutzeradministrator erfolgen.
<i>Kontrollinstanz</i>	Eine Kontrollinstanz, z. B. die EDV-Revision, unterzieht die Anträge regelmäßig einer Prüfung.
<i>Berichte</i>	Die Anträge und Benutzereinrichtungen werden elektronisch archiviert. Dies erlaubt die regelmäßige und automatische Auswertung aller vorhandenen Daten sowie die Erstellung von Sicherheitsreports im Rahmen des Security-Reporting.

10.2.3.2 Zugangsschutz

Das folgende Beispiel enthält eine prinzipielle Basisregel für den Zugangsschutz.



Basisregel Zugangsschutz

Der Zugang zu geschützten Informationssystemen, wird nur gewährt,
wenn sich der jeweilige Nutzer
(Person oder ein anderes Computersystem)
eindeutig identifiziert und authentisiert hat.

Aus der Basisregel kann folgende beispielhafte und auszugsweise Richtlinie zum Zugangsschutz abgeleitet werden, deren Phasen sich am später erläuterten Lebenszyklusmodell orientieren.



Richtlinie Zugangsschutz

Allgemeine und phasenübergreifende Vorgaben

1. Zugangsrechte werden nach dem „Prinzip der minimalen Rechte“ vergeben.
2. Die Vergabe von Zugangsrechten zu schützenswerten Objekten basiert auf Rollen.

3. Die Festlegung, Prüfung, Genehmigung, Einrichtung und Rücknahme von Rollen für die zu schützenden Objekte und von den ihnen zugeordneten fachlichen Zugangsrechten sowie Nutzungszeiten erfolgt gemäß dem „Antrags- und Genehmigungsverfahren Rollen“.
4. Die Beantragung, Prüfung, Genehmigung, Einrichtung und Rücknahme von Zugangsberechtigungen sowie die Aufbewahrung der Anträge erfolgt nach dem „Antrags- und Genehmigungsverfahren Zugang“. Die Vergabe und Rücknahme von Zugangsrechten werden dabei schriftlich dokumentiert. Die Dokumentation der vergebenen Zugangsrechte wird für die Dauer von 10 Jahren nach Ende bzw. Rücknahme der Zugangsrechte aufbewahrt.
5. Benutzerkonten, die nicht innerhalb eines Zeitraums von 30 Tagen nach Einrichtung genutzt werden, werden automatisch gesperrt.
6. Benutzerkonten, die über einen Zeitraum von 60 aufeinander folgenden Tagen nicht mehr genutzt wurden, werden automatisch gesperrt.
7. Beim Logon wird dem Benutzer zur Kontrolle die letzte erfolgreiche Anmeldung mit Datum und Uhrzeit angezeigt.
8. Der Zugang zum System wird zeitlich begrenzt, auf
 - die aufgabenspezifischen Arbeitstage,
 - die aufgabenspezifischen Arbeitszeiten.
9. Jeder Arbeitsplatzcomputer, wie z. B. PC und Notebook, verfügt über eine manuell oder automatisch auslösbare Sperre. Der Zugang zum Arbeitsplatzcomputer kann manuell gesperrt werden. Bei Windows®-Arbeitsplätzen erfolgt dies mittels der Tastenkombination „Strg+Alt+Entf“ und anschließendem Sperren des Computers. Der Zugang zu PCs und Notebooks wird nach einer vorgegebenen Zeit der Inaktivität (z. B. 5 Minuten) automatisch gesperrt. Die Reaktivierung eines PCs bzw. Notebooks nach der Sperrung darf nur nach Eingabe des erforderlichen Passworts erfolgen.
10. Sessions werden nach einer vorgegebenen Zeit der Inaktivität (z. B. 1h) automatisch abgebrochen (Zwangs-Logout).
11. ...

Planungsphase

1. Die zu schützenden Objekte bzw. Ressourcen (z. B. Netze, Computer, Anwendungen) werden in der Planungsphase identifiziert. Dann wird ihr Schutzbedarf erhoben und sie werden in Sicherheitsklassen eingeteilt.
2. ...

Fachkonzeptionsphase

1. Für die zu schützenden Objekte werden fachlich kompetente Objekt- bzw. Ressourceneigentümer und deren Stellvertreter benannt. Diese sind für die Definition der Rollen und der zugeordneten Zugangsrechte verantwortlich.

2. Die erstmalige Festlegung, Prüfung und Genehmigung von Rollen für die zu schützenden Objekte sowie von den ihnen zugeordneten fachlichen Zugangsberechtigungen sowie der Nutzungszeiten erfolgt zu Beginn der Fachkonzeptionsphase gemäß dem „Antrags- und Genehmigungsverfahren Rollen“. Rollen sind z. B. Administrator, Sachbearbeiter <Musteraufgabe> und Revisor.

3. ...

Technische Konzeptionsphase (Grob- und Feinkonzept)

1. Für die zu schützenden Objekte werden während der Technischen Konzeptionsphase je Rolle die fachlichen Zugangsberechtigungen in technische Zugangsberechtigungen überführt sowie weitere Rollen definiert, z. B. für Netz- und Datenbankadministratoren sowie technische Benutzer.

2. ...

Entwicklungsphase

1. In der Entwicklungsphase werden die Möglichkeiten zum späteren Anlegen der geforderten Rollen auf Basis der technischen Feinspezifikation realisiert.

2. ...

Testphase

(Integrations- und Systemtest einschließlich Freigabe und Abnahme)

1. Die Einrichtung der Rollen in der Testumgebung erfolgt gemäß dem „Antrags- und Genehmigungsverfahren Rollen“ mit Beginn der Testphase.
2. Die Beantragung, Prüfung, Genehmigung, Einrichtung und Rücknahme von Zugangsberechtigungen für die Testumgebung sowie die Aufbewahrung der Anträge erfolgt nach dem „Antrags- und Genehmigungsverfahren Zugang“.

3. ...

Inbetriebnahme- und Betriebsphase

1. Die Einrichtung der Rollen in der Produktionsumgebung erfolgt gemäß dem „Antrags- und Genehmigungsverfahren Rollen“ im Rahmen der Inbetriebnahme.
2. Die Beantragung, Prüfung, Genehmigung, Einrichtung und Rücknahme von Zugangsberechtigungen für die Produktionsumgebung sowie die Aufbewahrung der Anträge erfolgt nach dem „Antrags- und Genehmigungsverfahren Zugang“.
3. Der Bereich Informationsservices prüft die eingerichteten Benutzerkonten monatlich auf Nutzung. Bei Nichtnutzung erfolgt innerhalb von 5 Arbeitstagen die Klärung, ob das Benutzerkonto zu löschen oder zu sperren ist.

4. Der Bereich Informationsservices überprüft die vorhandenen Benutzerkonten zeitnah im Hinblick auf gesperrte Konten. Bei gesperrten Benutzerkonten erfolgt eine Klärung mit dem Benutzer. Bei Missbrauchsverdacht ergreift der Bereich Informationsservices umgehend geeignete Sicherheitsmaßnahmen.
5. ...

Außerbetriebnahmephase

1. Im Vorfeld der Außerbetriebnahme werden noch vorhandene Zugangsberechtigungen überprüft und deren Benutzer über die bevorstehende Außerbetriebnahme informiert. Nach erfolgreicher Abstimmung der Löschung werden die fachlichen Benutzer gelöscht.
2. ...

Eine prinzipielle und auszugsweise Richtlinie für Wireless LANs kann beispielsweise folgende Elemente beinhalten:

Richtlinie Wireless LAN

Planungsphase

1. Die Notwendigkeit eines WLANs ist zu prüfen.
2. Die Einrichtung eines WLANs ist schriftlich zu beantragen, zu begründen, vom Bereich Informationsservices zu prüfen und zu genehmigen bzw. abzulehnen.
3. Das WLAN ist gemäß der „Richtlinie Ressource WLAN“ zu planen.
4. ...

Technische Konzeptionsphase (Grob- und Feinkonzept)

1. In der technischen Konzeptionsphase sind das WLAN, seine Topologie, die Anbindung an andere Netze sowie die technischen Merkmale und geforderten Einstellungen zu spezifizieren.
2. ...

Implementierungsphase

1. Das WLAN ist gemäß Technischem Feinkonzept aufzubauen.
2. WLANs sind gemäß der „Richtlinie Ressource WLAN“ zu konfigurieren.
3. Die Konfiguration des WLANs, der Access Points und der Clients ist zu dokumentieren und vom Verantwortlichen abzuzeichnen.
4. ...

Testphase

(Integrations- und Systemtest einschließlich Freigabe und Abnahme)

1. Das WLAN, die Access Points und die WLAN-Clients sind auf Erfüllung der technischen Feinkonzeption und der Implementierungs-



vorgaben zu testen.

2. WLANs sind vor der Inbetriebnahme einem vertraulich dokumentierten Penetrationstest zu unterziehen. Eventuelle Schwachstellen sind vor Inbetriebnahme zu beheben.
3. ...

Inbetriebnahme- und Betriebsphase

1. Die Protokolle (logs) sind regelmäßig auszuwerten.
2. Sicherheitsrelevante Firmware-Upgrades sind während der Betriebsphase nach vorherigem Test zeitnah einzuspielen.
3. Änderungen in der Konfiguration des WLANs darf nur der Bereich Informationsservices vornehmen.
4. Nach Konfigurationsänderungen ist die neue Konfiguration zu dokumentieren und vom Verantwortlichen abzuzeichnen sowie für 10 Jahre ab dem Tag der dokumentierten folgenden Konfigurationsänderung aufzubewahren.
5. WLANs sind jährlich einem vertraulich dokumentierten Penetrationstest zu unterziehen. Über eine zumindest temporäre Außerbetriebnahme bei Entdeckung einer oder mehrerer Schwachstellen ist sofort zu entscheiden und die Entscheidung umzusetzen. Eventuelle Schwachstellen sind umgehend zu beheben.
6. ...

10.2.3.2.1 Identifikation

Das folgende prinzipielle Beispiel enthält eine auszugsweise Richtlinie zur Benutzererkennung.



Richtlinie Benutzererkennung

1. Jeder Nutzer erhält vom Bereich Informationsservices eine eindeutige Benutzererkennung (UserId). Eineindeutig bedeutet umkehrbar eindeutig, so dass jedem Benutzer eindeutig eine Benutzererkennung zugeordnet ist und umgekehrt anhand der Benutzererkennung der Rückschluss auf den Benutzer möglich ist, um die Nachvollziehbarkeit der Aktivitäten zu ermöglichen.
2. Im System voreingestellte Benutzerkennungen sind durch den Administrator zeitnah zu ersetzen und zu löschen.
3. Jeder Benutzer darf nur die ihm zugeordnete(n) Benutzererkennung(en) nutzen und diese nicht weitergeben.
4. Benutzer dürfen ihre Benutzerkennungen nicht speichern, z. B. in einem Login-Makro, in einer Datei oder in einem Login-Manager.
5. ...

10.2.3.2.2 Authentisierung – Passwortregeln

Im Folgenden sind beispielhaft Passwortregeln in Form von Passwortge- und -verboten sowie -eigenschaften und -prüfungen angegeben.

In der folgenden Liste sind auszugsweise und beispielhaft Passwortregeln in Form von Passwortgeboten angegeben.

Passworte

Gebote

1. Bei vorinstallierten Benutzern müssen die Standardpasswörter geändert werden. Die gesicherte Verfügbarkeit der geänderten Passwörter ist sicherzustellen.
2. Bei der Anforderung eines Ersatzpasswortes ist die Identität des Anfordernden sicher zu verifizieren.
3. Das Erstpasswort ebenso wie Ersatzpasswörter sind dem Benutzer vertraulich zu übermitteln. Die Identität des Empfängers ist sicherzustellen.
4. Der Empfang des Passwortes ist vom Benutzer schriftlich zu bestätigen.
5. Das Erstpasswort ebenso wie Ersatzpasswörter sind beim ersten Login zu ändern.
6. Die Eingabe des Passworts muss unbeobachtet erfolgen.
7. Der Benutzer muss das Passwort vertraulich behandeln. Es darf nur ihm bekannt sein.
8. Bei Bekanntwerden ist das Passwort sofort zu ändern.
9. Die Änderung des Passworts muss bei Schutzobjekten der Vertraulichkeitsstufen T3 und T4 nach jeweils 30 Tagen erfolgen, bei den niedrigeren Vertraulichkeitsstufen nach 90 Tagen.
10. Die Länge des Passworts muss bei Standardbenutzern 8 Stellen, bei privilegierten Benutzern 10 Stellen betragen.
11. Die im Passwort verwendeten Zeichen müssen Buchstaben und Ziffern sowie – wenn technisch unterstützt – Sonderzeichen sein.
12. ...

Das folgende Beispiel enthält eine beispielhafte Liste von Passwortverboten.

Passworte

Verbote

1. Umgang mit dem Passwort
2. Notiz- und Speicherverbot: Das Passwort darf nicht notiert werden (Ausnahme: Notfallpasswort bei Hinterlegung in verschlossenem Um-

schlag im Safe). Dies beinhaltet, dass der Benutzer Passwörter auch nicht auf Funktionstasten legen oder anderweitig speichern darf, z. B. in Dateien, Datenbanken, Login-Makros, Anwendungen und Passwort-Managern.

3. Mitteilungsverbot: Passwörter dürfen Dritten nicht mitgeteilt oder zur Kenntnis gebracht werden.
4. Wiederholungsverbot: Geschäftlich verwendete Passwörter dürfen nicht außerhalb des Geschäftsbetriebs eingesetzt werden. Dasselbe Passwort darf nach Ablauf innerhalb eines Zeitraums von 14 Monaten nicht wieder verwendet werden. Korruptierte Passwörter dürfen nicht wieder verwendet werden. (Dies erfordert eine Historienführung der Passwörter im Computersystem. Bei einer Historisierung über ein Jahr und ca. 30täglichem Passwortwechsel ergeben sich ca. 13 Passwörter.)
5. Verbot der Mehrfachänderung: Die Mehrfachänderung des Passworts innerhalb kurzer Zeit zur Umgehung des Wiederholungsverbots ist verboten.
6. ...

Die folgende Liste enthält beispielhaft Passwortheigenschaften.



Passworte

Passwortheigenschaften

1. Verbot von Trivialpasswörtern. Folgende Passwortarten dürfen nicht verwendet werden:
 - Kein Passwort (Return-Taste),
 - Lexikalisch ermittelbare Passwörter, egal aus welcher Sprache, z. B. „Passwort“, „password“, „Benutzer“, „user“, „Gast“, „guest“,
 - Gleiche Zeichen, z. B. ZZZZZ,
 - Aufeinander folgende Ziffern z. B. 123456,
 - Bekannte Ziffernfolgen, z. B. 0815, 4711,
 - Datum (z. B. Geburtsdatum {eigenes, aus der Familie, aus dem Freundes- oder Verwandtenkreis, berühmter Persönlichkeiten}, bekannter Ereignisse),
 - Nebeneinander liegende Tasten, z. B. asdf,
 - Name, Bezeichnung (z. B. Vorname, Nachname {eigener/aus der Familie/aus dem Freundes- oder Verwandtenkreis}, Spitzname, Name aus einem Namenslexikon, Name des Haustiers, Namen von Autoren, Fernsehstars, Fernsehsendungen, Ländern, Orten, Gebäuden, Computern, Autos, Herstellern, Produkten, Buchtitel, Filmtitel),
 - Sprichwörter, Aussprüche,
 - Kfz-Kennzeichen,
 - Kombinationen benachbarter Tasten,
 - Bereits genutzte Passwörter.
2. ...

Das folgende Beispiel enthält prinzipiell mögliche Anforderungen zur Passwortprüfung.

Passworte

Passwortprüfung

1. Die Passwortstärke ist durch den Bereich Informationsservices mittels eines geeigneten Tools monatlich zu prüfen. Verstöße gegen die Passwortregeln sind dem Benutzer, seinem Vorgesetzten und dem IT-Sicherheitsbeauftragten mitzuteilen.
2. ...



10.2.3.2.3 Computerviren-Schutz

Das folgende Beispiel zeigt prinzipielle Eckpunkte einer Richtlinie zum Schutz vor Computerviren.

Richtlinie Computerviren-Schutz

1. Jeder Rechner (Arbeitsplatzrechner, Server, Firewall) wird mit einem Viren-Suchprogramm ausgestattet.
2. Zugänge zum Unternehmensnetz werden mit Viren-Suchprogrammen abgesichert.
3. Der Virens Scanner wird täglich auf dem zentralen Server automatisch aktualisiert.
4. Die Virens Scanner der Clients werden zum nächstmöglichen Zeitpunkt aktualisiert.
5. Virens Scanner werden so konfiguriert, dass sie resident sind, d. h. sie werden beim Start des Rechners in den Speicher geladen und verrichten ihre Aufgabe im Hintergrund ohne Zutun des Benutzers.
6. Virens Scanner werden so eingestellt, dass auch eingehende und zur Versendung anstehende E-Mails sowie deren Anhänge überprüft werden.
7. Virenbehaftete eingehende E-Mails werden isoliert und der Empfänger benachrichtigt.
8. Jeder Mitarbeiter meldet einen Virenverdacht umgehend an die Hotline.
9. ...



10.2.3.3 Zugriffsschutz

Eine Richtlinie für den Zugriffsschutz kann beispielsweise folgende Inhalte aufweisen.



Richtlinie Zugriffsschutz

Allgemeine und phasenübergreifende Vorgaben

1. Zugriffsrechte werden nach dem Prinzip der „minimalen Rechte“ vergeben, d. h. Zugriffsberechtigungen werden nur in dem Maße erteilt, wie sie zur Aufgabenerfüllung minimal erforderlich sind.
2. Es werden frühestmöglich Rollen festgelegt, denen Zugriffsberechtigungen zugeordnet werden.
3. Für die Beantragung und Vergabe von Zugriffsberechtigungen wird das „Antrags- und Genehmigungsverfahren Zugriffsberechtigung“ mit dem dazugehörigen Antragsdokument verwendet.
4. Für Systeme, Anwendungen und Datenbestände werden Eigentümer und Stellvertreter benannt, die für die Definition von Rollen und zugeordneten Zugriffsberechtigungen verantwortlich sind.
5. ...

Fachkonzeptionsphase

1. In der Fachkonzeptionsphase legt die Fachabteilung die Rollen fest, die – z. B. zur Erfüllung gesetzlicher oder aufsichtsbehördlicher Anforderungen – aus fachlicher Sicht erforderlich sind, und ordnet diesen Zugriffsberechtigungen zu.
2. ...

Technische Konzeptionsphase (Grob- und Feinkonzept)

1. In der technischen Konzeptionsphase transformiert der Bereich Informationsservices die fachlichen Anforderungen in technische Anforderungen.
2. ...

Implementierungsphase

1. In der Implementierungsphase realisiert der Bereich Informationsservices die Anforderungen aus dem technischen Feinkonzept.
2. ...

Testphase

(Integrations- und Systemtest einschließlich Freigabe und Abnahme)

1. In der Testphase prüfen Tester die Erfüllung der technischen Anforderungen (Verifikation) und der fachlichen Anforderungen (Validierung).
2. ...

Inbetriebnahme- und Betriebsphase

1. Für die Beantragung und Vergabe von Zugriffsberechtigungen wird das „Antrags- und Genehmigungsverfahren Zugriffsberechtigung“ mit dem dazugehörigen Antragsdokument verwendet.
2. Die Zugriffsberechtigungen für Mitarbeiter werden unter Angabe der Rolle des jeweiligen Mitarbeiters von der Personalabteilung beantragt.
3. Die beantragten Zugriffsberechtigungen werden von der jeweiligen Führungskraft geprüft.
4. Die Berechtigungsanträge werden vom Ressourceneigentümer genehmigt bzw. abgelehnt.
5. Die Zugriffsberechtigungen werden von den zuständigen Administratoren eingerichtet und die Berechtigungsanträge archiviert.
6. ...

Außerbetriebnahmephase

1. Im Vorfeld der Außerbetriebnahme werden noch vorhandene Zugriffsberechtigungen überprüft und deren Benutzer über die bevorstehende Außerbetriebnahme informiert. Nach erfolgreicher Abstimmung der Löschung werden die Zugriffsberechtigungen in der Regel gemeinsam mit der Benutzerkennung gelöscht.
2. ...

10.2.3.4 Leseschutz

Eine Richtlinie für den Leseschutz kann beispielsweise folgende Elemente beinhalten:

Richtlinie Leseschutz

1. Vertrauliche Daten auf Notebooks sind verschlüsselt zu speichern.
2. Über öffentliche Netze übertragene vertrauliche Informationen sind zu verschlüsseln.
3. Auf mobilen Datenträgern, z. B. Memory Sticks, CD-ROMs, Datenbändern und mobilen Festplatten, gespeicherte vertrauliche Daten sind zu verschlüsseln.
4. Bei Providern gespeicherte vertrauliche Daten sind verschlüsselt sowohl zu übertragen als auch zu speichern.
5. Gegen den Verlust des geheimen Schlüssels sind geeignete Maßnahmen vorzusehen.
6. ...



10.2.3.5 Protokollierung/Beweissicherung

Die Richtlinie für die Protokollierung sicherheitsrelevanter Ereignisse kann überblicksartig in Form einer Matrix dargestellt werden, wie das folgende prinzipielle Beispiel zeigt:

Sicherheitsklasse	Protokollierung				
	Zugang		Datenzugriff		
	Logon	Logoff	Schreibend	Lesend	...
Hoch	Alle	Alle	Alle	Alle	...
Mittel	Alle	Alle	Alle	Keine	...
Niedrig	Alle	Alle	Keine	Keine	...

Für diese sicherheitsrelevanten Ereignisse sind die Daten zu definieren, die protokolliert werden sollen. Darüber hinaus ist festzulegen, wie diese Daten gesichert und archiviert werden und wer diese Daten einsehen darf. Dies kann in Form einer Tabelle wie folgt dargestellt werden:

Ergebnis										
Recht										
Objekt										
Terminalkennung										
Uhrzeit										
Datum										
Benutzerkennung										
Ereignis										
Schutzelement									Auswertungs- berechtigung	Auswer- tungs- zyklus
Zufahrt	X	X	B	B	X	X	X	X	A, R	t, m
Zutritt	X	X	B	B	X	X	X	X	A, R	t, m
Zugang	X	X	B	B	X	X	X	X	A, R	t, m
Ext. Zugang	X	X	B	B	X	X	X	X	A, R	t, m
Zugriff	X	X	X	X	X	X	X	X	A, R	t, m
Legende:										
X = Ereignis ist zu protokollieren,										
B = Beginn und Ende sind zu protokollieren, z. B. Einfahrt – Ausfahrt										
A = Administrator, R = Revisor, t = täglich, m = monatlich										

10.3 Ressourcen

10.3.1 Zutrittskontrollsystem

Das folgende prinzipielle Beispiel zeigt auszugsweise eine Richtlinie Zutrittskontrollsystem.

Richtlinie Zutrittskontrollsystem

1. Das Zutrittskontrollsystem ist an die Notstromversorgung anzuschließen.
2. Das Zutrittskontrollsystem muss Benutzerkennung, Zutrittsort, Datum und Uhrzeit sicher speichern bzw. übermitteln.
3. ...



10.3.2 Passwortspezifische Systemanforderungen

Aus den obigen Passwortge- und -verbotten ergeben sich Anforderungen an die zugrunde liegenden ITK-Systeme. Im Folgenden sind derartige Systemanforderungen angegeben:

Passwortspezifische Systemanforderungen

1. Nicht lesbare Anzeige des eingegebenen Passworts
2. Systemunterstützte Prüfung der Passwortregeln:
 - Trivialpasswörter einschließlich nur „RETURN“
 - Lexikalisch analysierbare Passwörter
3. Jederzeitige Änderbarkeit des Passworts
4. Wechselzwang nach vorgegebenem Intervall bzw. für Erstpasswort und Ersatzpasswörter
5. Historienführung der Passwörter (mindestens 14 Passwörter)
6. Zweimalige Eingabeaufforderung bei Passwortänderungen zur Verifikation
7. Sperrung bei mehrmaliger Fehleingabe (Anzahl einstellbar) und Meldung an den Systemadministrator
8. Einweg-verschlüsselte Speicherung der Passwörter
9. Übertragung von Passwörtern
 - Verschlüsselte Übertragung der Passwörter und Einmaligkeit der übertragenen Authentifizierungsinformation
 - Bei unverschlüsselter Übertragung von Passwörtern (nur zulässig bei niedrigen Sicherheitsanforderungen) sollten Einmalpasswörter verwendet werden
 - Um ein Mitschneiden und Wiedereinspielen (Replay) zu verhindern, sollten die verschlüsselt/unverschlüsselt übertragenen Passwörter einen variablen Anteil, z. B. aus Datum und Uhrzeit enthalten
10. Protokollierung von Passwortänderungen sowie von falschen Passworteingaben mit Anschluss, Benutzerkennung, Datum und Uhrzeit
11. ...



10.3.3 Wireless LAN

Eine prinzipielle und auszugsweise Richtlinie für die Ressource Wireless LAN kann u. a. beispielsweise folgende Elemente beinhalten:



Richtlinie Ressource Wireless LAN

Planungsphase

1. WLAN-Funkzellen sind so zu planen und anzuordnen, dass die Abstrahlleistung außerhalb des Gebäudes minimiert ist. Der Einsatz abstrahlungsdämmender Folien oder Fenster ist zu prüfen.
2. Die WLAN-Funkzellen sind so zu planen, dass die Abstrahlung innerhalb der Funkzelle möglichst gleichmäßig erfolgt und Funklöcher vermieden werden. Bei der Planung sind die dämpfende Wirkung von Stahl, stahlarmiertem Beton und Metalltüren, wie z. B. Brandschutztüren, zu berücksichtigen.
3. In der Planungsphase ist zu berücksichtigen, dass der Access Point an einer Wand oder der Decke angebracht oder zumindest erhöht aufgestellt werden sollte.
4. In der Planungsphase ist zu berücksichtigen, dass das WLAN als unsicheres Netz zu betrachten ist. Eine Anbindung des WLANs an das interne Netz erfolgt über einen Firewall und ein Intrusion Detection/Prevention System.
5. WLANs sind so zu planen, dass sie auf IEEE 802.11i, d. h. WPA2, basieren.
6. WLAN-Clients sind dahingehend zu planen, dass sie mit Firewall, zeitnah aktualisiertem Virenschanner und Verschlüsselung ausgestattet werden.
7. ...

Implementierungsphase

1. Der standardmäßig eingestellte Service Set Identifier (SSID) des Access Points ist zu ändern.
2. Der SSID-Broadcast des Access Points ist auszuschalten.
3. Der Access Point ist im Closed-Network-Modus zu betreiben.
4. Das Standard-Passwort für die Konfiguration des Access Points ist zu ändern.
5. Die Konfiguration des Access-Points ist auf spezifische Clients aus dem LAN zu beschränken.
6. Am Access Point ist die MAC-Adressfilterung zu aktivieren.
7. Das WLAN muss auf IEEE 802.11i, d. h. WPA2, basieren.
8. Die Verschlüsselung ist zu aktivieren.
9. Am Access Point ist DHCP (Dynamic Host Configuration Protocol) zu deaktivieren, das die dynamische Zuweisung von IP-Adressen ermöglicht.
10. Die Protokollierung (logging) ist einzuschalten.
11. WLAN-Clients sind mit Firewall, zeitnah aktualisiertem Virenschanner und Verschlüsselung auszustatten.
12. ...

10.4 Organisation

Die folgende Matrix zeigt ein prinzipielles überblicksartiges und auszugswises Beispiel zu verschiedenen Rollen im Rahmen des Sicherheitsmanagements, zu denen u. a. Rollen aus den Prozessen, wie z. B. Risk -, Problem -, Change -, Configuration -, Security -, Notfallmanager, hinzukommen.

Funktion, Rolle													
													...
													Werkschutz
													System-Administratoren
													EDV-Revisoren
													Sicherheitsauditoren
													Dezentraler Sicherheitsbeauftragter
													Zentraler Sicherheitsbeauftragter
													Produktionsverantwortlicher
													Entwicklungsverantwortlicher
													Datenverantwortlicher
													Datenschutzbeauftragter
													Nutzer, Endanwender
													Geschäftsbereichsleiter
													Geschäftsleiter
Tätigkeit													
Sicherheitspolitik definieren, pflegen	V	M		M					M			M	
Sicherheitsziele festlegen und pflegen		V	M	M					M			M	
Sicherheitsklassen bilden und pflegen		M	M					M	V				
SSFD durchführen und pflegen							M	M	V				
Sicherheitsarchitektur konzip., pflegen							M	M	V				
Si.-Richtlinien entwickeln, pflegen							M	M	V				
Spezifische Sicherheitskonzepte erstellen und pflegen							M	M	V	M			
ITK-Systeme sicher entwickeln							V						
ITK-Systeme sicher betreiben								V					
Rollen festlegen						V							
Sicherheitsadministration (Zugangs- und Zugriffsschutz) durchführen und Anträge archivieren												V	
Datenschutz wahrnehmen				V									
Audits durchführen										V			
Prüfungen durchführen											V		
Sicherheitsadministration (Zutrittsschutz) durchführen													V
Objekt schützen													V
...													
Legende: V = verantwortlich, M = mitwirkend													

10.5 Zusammenfassung

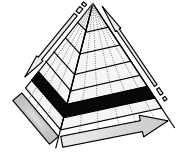
Richtlinien bilden eine systemübergreifende Basis für ein Sicherheits-, Kontinuitäts- und Risikomanagement, das auf Systematik und auf ein anforderungsbezogen vergleichbares Sicherheitsniveau ausgerichtet ist. Grundsätzlich lassen sich für alle Prozesse und Ressourcen sowie für den Lebenszyklus Richtlinien erstellen. Sie können sich z. B. auf den Zufahrts-, Zutritts-, Zugangs-, Zugriffs- und Leseschutz beziehen, Standards für die Prozessdokumentation vorgeben und Regeln für Firewalls, Intrusion-Detection-Systeme, Spam-Filter und die Absen-dekontrolle festlegen.

Die vorangegangenen Unterkapitel enthalten prinzipielle und aus-zugsweise Beispiele für Sicherheitsregeln, Prozessvorlagen, IT-Benutzerordnung, E-Mail-Nutzung, Datensicherung, Notfall- und Katastrophenvorsorge und Berichtswesen sowie verschiedene The-men des Sicherheits- und Kontinuitätsmanagements.

Richtlinien können die Effizienz fördern, da dieselben Themen, wie z. B. die Durchführung einer Schutzbedarfsanalyse, und deren Inhal-te, die Erstellung von Notfall- und Katastrophenvorsorge- bzw. BCM-Handbüchern/Portalen oder die Passwortregeln bereits prozess- und ressourcenübergreifend als Rahmen festgelegt sind.

11 Spezifische Sicherheitskonzepte

Spezifische Sicherheitskonzepte sind in Unternehmen häufig anzutreffen. Sie beschreiben z. B., welche Sicherheitseinstellungen für ein bestimmtes Betriebssystem getroffen werden sollen. Doch erfüllen diese Sicherheitskonzepte die gestellten Anforderungen? Und wenn ja, ist dies angemessen und nachvollziehbar?



Die Angemessenheit und Nachvollziehbarkeit der spezifischen Sicherheitskonzepte kann dadurch erreicht werden, dass

- die zugrunde gelegten Anforderungen und Richtlinien referenziert werden
- die Risikostrategie im Hinblick auf Vermeidung, Verringerung, Verlagerung oder Vereinnahmung des Risikos dargestellt wird
- die zu treffenden Maßnahmen beschrieben werden.

Wie die Verbreiterung der Sicherheitspyramide veranschaulicht, nimmt mit jeder tieferen hierarchischen Ebene der Detaillierungsgrad und aufgrund der Heterogenität und Spezifität auch die Anzahl der jeweiligen Konzepte und Maßnahmen zu. Gleichzeitig steigt die Änderungshäufigkeit. Die Konzeptentwicklung auf dieser Ebene der Sicherheitspyramide obliegt in den Unternehmen Spezialisten, wobei zur Umsetzung der Richtlinien in spezifische Konzepte die jeweils prozess- oder ressourcenspezifischen Dokumentationen genutzt werden. Daher konzentriert sich dieses Kapitel auf wenige prinzipielle und auszugsweise Konzeptbeispiele. Untergliedert ist es in

1. Prozesse
2. Ressourcen
3. Zusammenfassung

11.1 Prozesse

11.1.1 Kontinuitätsmanagement

11.1.1.1 Datensicherung

Dokumentationsvorlage Datensicherung			
	Datenbestand 1	...	Datenbestand n
Verantwortlich	Ralf Mustermann		Fritz Mustermann
Stellvertreter	Heinz Muster- mann		Horst Mustermann
Datentyp	ABC-Daten der Anwendung x		Anwendungspro- gramm y
Datensicherungstool	Mustertool 1, Release 2.2		Mustertool 2, Release 1.8
Medium	DLT-Bandkassette		DLT-Bandkassette
Aktivierungsart	Zeit		Ereignis
Aktivierungsanstoß	Automatisch		Manuell
Generation 1	5 Mediasets		1 Mediaset
Sicherungszeitpunkt	Mo – Fr., 23:00		Releasewechsel
Sicherungsumfang	Inkrementell		Komplett
Archivierungslokation	Serverraum		Datensicherungs- archiv
Archivierungsdauer	1 Woche		10 Jahre ab Folge- Releasewechsel
Generation 2	5 Mediasets		
Sicherungszeitpunkt	Sa, 22:00		
Sicherungsumfang	Komplett		
Archivierungslokation	Datensicherungs- archiv		
Archivierungsdauer	5 Wochen		
Generation 3	12 Mediasets		
Sicherungszeitpunkt	Letzter Tag im Monat, 22:00		
Sicherungsumfang	Komplett		
Archivierungslokation	Datensicherungs- archiv		
Archivierungsdauer	1 Jahr		
Generation 4	10 Mediasets		
Sicherungszeitpunkt	1. Januar, 0:30		
Archivierungslokation	Datensicherungs- archiv		
Archivierungsdauer	10 Jahre		
Sicherungsumfang	Komplett		

11.2 Ressourcen

11.2.1 Betriebssystem

11.2.1.1 Systemspezifische Passworteinstellungen

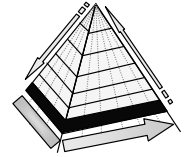
Systemspezifische Passworteinstellungen für Musterbetriebssystem		
Systemanforderung	Parameter-name	Wert/ Bemerkung
1. Nicht lesbare Anzeige des eingegebenen Passwortes		✓
2. Systemunterstützte Prüfung der Passwortregeln: – Trivialpasswörter einschließlich nur „RETURN“ – Lexikalisch analysierbare Passwörter		✓ ✓
3. Jederzeitige Änderbarkeit des Passworts		✓
4. Wechselzwang nach 30 Tagen bzw. für Erstpasswort	...	30
5. Historienführung der Passwörter (Einstellung: 13 PW)	...	13
6. Zweimalige Eingabeaufforderung bei Passwortänderungen zur Verifikation		✓
7. Sperrung bei dreimaliger Fehleingabe und Meldung an den Systemadministrator	...	3 ✓
8. Einweg-verschlüsselte Speicherung der Passwörter		✓
9. Übertragung von Passwörtern (PW) – Verschlüsselte Übertragung der PW und Einmaligkeit der übertragenen Authentifizierungsinformation		✓
10. Protokollierung von PW-Änderungen sowie von falschen PW-Eingaben mit Anschluss, UserId, Datum und Uhrzeit		✓
11. ...		

11.3 Zusammenfassung

Die vorangegangenen auszugsweisen Beispiele und Hilfsmittel zeigen, dass die Richtlinien mit überschaubarem Aufwand als Basis für Konzepte und Prüfungen genutzt werden können.

12 Sicherheitsmaßnahmen

Die erstellten Sicherheitskonzepte müssen in den jeweiligen ITK-Systemen implementiert werden. Hierzu werden die in den Konzepten beschriebenen Maßnahmen durchgeführt und protokolliert. So kann z. B. die Konfiguration, die Parametrisierung und die Löschung von Standardbenutzern in den Informationssystemen nachvollziehbar dokumentiert werden. Alternativ hierzu können Ausdrücke der jeweiligen Systemeinstellungen als Dokumentation verwendet werden.



Im Folgenden ist beispielhaft angegeben, wie ein solches manuell gepflegtes Protokoll aussehen kann.

1. Ressourcen
2. Zusammenfassung

12.1 Ressourcen

12.1.1 Betriebssystem: Protokoll Passwordeinstellungen

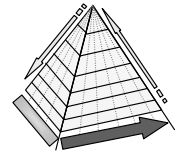
Protokoll der Passwordeinstellungen für <Musterbetriebssystem> für den Server <Serveridentifikator> am Standort <Standort>		
Systemanforderung	Parametername und Wert	Ok (✓) / Bemerkung
1. Wechselzwang nach 30 Tagen bzw. für Erstpasswort	... = 30	✓
2. Historienführung der Passwörter (Einstellung: 13 Passwörter)	... = 13	✓
3. Sperrung bei dreimaliger Fehl- eingabe und Meldung an den Systemadministrator	... = 3	✓
...	...	
Einstellung vorgenommen am: <Datum> von <Name, Vorname> Unterschrift: <Unterschrift>		

12.2 Zusammenfassung

Die Systemeinstellungen sind über die Sicherheitsrichtlinien und die prozess- und ressourcenspezifischen Konzepte definiert. Im Rahmen der Sicherheitsmaßnahmen werden sie in dem jeweiligen Prozess bzw. der jeweiligen physisch vorhandenen Ressource realisiert. Ihre Dokumentation kann sowohl manuell als auch durch Ausdruck und Abzeichnung der entsprechenden Dokumentation erfolgen.

13 Lebenszyklus

Die vorangegangenen Kapitel haben gezeigt, wie das Sicherheits-, Kontinuitäts- und Risikomanagement mittels der Sicherheitspyramide aufgebaut wird. Ausgangspunkt ist die Sicherheits-, Kontinuitäts- und Risikopolitik gewesen von der aus wir schrittweise bis hin zu den Maßnahmen gelangt sind. Doch wann sind die dort definierten Sicherheitselemente zu berücksichtigen?



Der Fokus der ITK-Sicherheit in Unternehmen liegt häufig auf dem sicheren Betrieb der Informationssysteme. Sicherheitsdefizite im Betrieb oder bei der Einführung in den Betrieb haben jedoch oftmals Ursachen, die in früheren Phasen des Lebenszyklus von Prozessen, Ressourcen oder Organisation zu suchen sind. Dieses Kapitel zeigt dies beispielhaft am Lebenszyklus eines Informationssystems und unter Nutzung eines exemplarischen Phasenmodells. Die Ausführungen lassen sich in analoger Form übertragen auf andere Phasenmodelle, andere Ressourcen sowie auf Prozesse, Produkte und Dienstleistungen.

Schon die Beantragung eines Informationssystems erfordert die Betrachtung der Sicherheitsanforderungen, da sie sowohl auf die Anschaffungs- und Entwicklungs- als auch Betriebskosten Einfluss haben. Beispielsweise müssen der Schutzbedarf einschließlich der Verfügbarkeit eines Informationssystems, die Kapazitäts- und Performanceanforderungen und deren -entwicklung sowie die verschiedenen Benutzerrollen ermittelt werden. In späteren Phasen müssen diese Anforderungen schrittweise verfeinert, umgesetzt und getestet werden. Dies zeigt, dass in allen Phasen des Lebenszyklus Sicherheitsaspekte zu berücksichtigen sind.

Darüber hinaus begleiten alle in der Sicherheitsarchitektur genannten Managementdisziplinen den Lebenszyklus eines Prozesses, einer Ressource, eines Produkts oder einer Dienstleistung, haben Schnittstellen zu ihm und sind daher zu berücksichtigen.

Einige Sicherheitselemente und sicherheitsspezifische Schnittstellen sind in den folgenden Unterkapiteln, den Phasen im Lebenszyklus eines ITK-Systems, dargestellt:

1. Beantragung
2. Planung
3. Fachkonzept, Anforderungsspezifikation
4. Technisches Grobkonzept

5. Technisches Feinkonzept
6. Entwicklung
7. Integrations- und Systemtest
8. Freigabe
9. Software-Evaluation
10. Auslieferung
11. Abnahmetest und Abnahme
12. Software-Verteilung
13. Inbetriebnahme
14. Betrieb
15. Außerbetriebnahme
16. Hilfsmittel Phasen-Ergebnistypen-Tabelle
17. Zusammenfassung

13.1 Beantragung

Bei der Beantragung eines Informationssystems müssen Sicherheitsanforderungen zumindest überblicksartig betrachtet werden. Sie haben Einfluss sowohl auf die Anschaffungs- und Entwicklungs- als auch die Betriebskosten. Dies betrifft beispielsweise die Anforderungen an die Verfügbarkeit und die Sicherheit des Systems. Soll das Informationssystem später unterbrechungsfrei „rund um die Uhr“ zur Verfügung stehen oder sind Ausfallzeiten und wenn ja, in welcher Länge akzeptabel? Gibt es spezielle Anforderungen, z. B. an die Vertraulichkeit der Daten, die eine Verschlüsselung erforderlich machen? Können Fehlfunktionen des Informationssystems zu Personenschäden führen?

Ferner sind erste Angaben zum Mengengerüst erforderlich, z. B.:

- Welches Datenvolumen wird erwartet?
- Wie wird sich das Datenvolumen zukünftig entwickeln?
- Wie viele Benutzer wird es geben?
- In welchem Umfang werden diese das Informationssystem nutzen?
- Über welchen Zeitraum soll das Informationssystem genutzt werden?
- Welchem Nutzen stehen welche Kosten für Entwicklung und Betrieb gegenüber?

13.2 Planung

Bei der Planung eines ITK-Systems ist zu berücksichtigen, dass in den Phasen des Lebenszyklus Sicherheitskonzepte und -maßnahmen entwickelt und später geprüft werden müssen. Außerdem sind prozessuale, ressourcenspezifische, z. B. technologische, methodische und personelle, sowie organisatorische Aspekte (PROSim) zu beachten. Hierzu gehört beispielsweise die Sicherheit der Entwicklungs- und der späteren Betriebsumgebung, die Funktionstrennung zwischen Entwicklung, Test und Qualitätssicherung sowie die Sicherheitsanforderungen an die Prozesse, Ressourcen und Beteiligten.

13.3 Fachkonzept, Anforderungsspezifikation

In der Fachkonzeptionsphase erstellt der Fachbereich die fachliche Spezifikation und verfeinert die bereits überblicksartig erhobenen Sicherheitsanforderungen der vorherigen Phase. Die fachliche Spezifikation beinhaltet auch die Angabe von Schnittstellen, z. B. zu anderen ITK-Systemen.

*Schutzbedarfs-
analyse*

Der Security Manager – verantwortlich für den Prozess Security Management – unterstützt den Fachbereich und dokumentiert die Sicherheitsanforderungen oder auch Sicherheitsziele mittels der bereits beschriebenen standardisierten Schutzbedarfsanalyse. Anschließend bindet er aus der Organisationseinheit Informationsservices die ITK-Systementwicklung und den ITK-Betrieb mit ein. Diese bringen ihre Erfahrung aus Entwicklung und Betrieb ein und schätzen Dauer und Kosten für die Realisierung der Sicherheitsanforderungen im Hinblick auf PROSim ab.

Entsprechend den Ergebnissen der Schutzbedarfsanalyse klassifiziert der Security Manager das Informationssystem. Hierbei berücksichtigt er die primären Sicherheitskriterien Konformität, Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie die sekundären Sicherheitskriterien Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit. Zusätzlich zur Klassifizierung des Gesamtsystems sollten gegebenenfalls die einzelnen spezifizierten Komponenten ebenfalls aus fachlicher Sicht klassifiziert werden, um spätere Tests und Sicherheitsmaßnahmen darauf ausrichten zu können.

*Sicherheits-
klassifizierung*

Neben dem Fachkonzept (Lastenheft) mit den funktionalen und datentechnischen Anforderungen liegen als Ergebnis dieser Phase der Schutzbedarf und die Sicherheitsklasse vor. Dies beinhaltet u. a. die Konsequenzen bei Verletzung der Sicherheitskriterien, rechtliche

Ergebnis

Qualitäts- sicherung

Anforderungen, wie z. B. den Datenschutz, ferner das Zugangs- und Zugriffsberechtigungs- bzw. Rollenkonzept sowie die Archivierungsanforderungen. Günstig ist es, wenn die Anforderungen eindeutig identifizierbar sind, z. B. über ein Nummernschema. Außerdem sollten sie mess- bzw. prüfbar sein, um die Erfüllung der Anforderungen verifizieren zu können.

Das Review-Team führt die Qualitätssicherung durch. Es setzt sich zusammen aus dem Sicherheitsbeauftragten, dem Qualitätsmanagementbeauftragten, Mitarbeitern der Fachabteilung, der Revision, der Software-Entwicklung und dem Betrieb. Das Review-Team prüft das Fachkonzept daraufhin, dass es vollständig, korrekt, konsistent und verständlich ist. Die Vollständigkeitsprüfung bezieht sich z. B. auch darauf, dass die Daten an den Schnittstellen des Systems fachlich genau beschrieben sind. Das schließt neben dem Datentyp auch die Angabe von fachlich begründeten zulässigen Werten, Wertebereichen, Grenzwerten und Zeichen sowie Feldlängen ein. Bereits an dieser Stelle ist darauf zu achten, dass Werte oder Zeichen, die sich später für Angriffe, z. B. SQL Injections, nutzen lassen, möglichst nicht zu den zulässigen Werten bzw. Zeichen gehören.

Das freigegebene Fachkonzept stellt der Konfigurationsmanager als Konfigurationselement (Configuration Item) in die Konfigurationsdatenbank (Configuration Management Database {CMDB}) ein.

13.4 Technisches Grobkonzept

Sicherheits- transformation

Das technische Grobkonzept überführt die fachlichen Anforderungen in technische, beispielsweise mittels der bereits beschriebenen Sicherheitstransformation. Hierbei entsteht ein erstes Systemkonzept, in dem die erforderlichen Hard- und Softwarekomponenten sowie die internen und externen Schnittstellen und deren Zusammenspiel dargestellt sind. Das Systemkonzept berücksichtigt hierbei Aspekte der Betriebssicherheit (Safety), der Kontinuität (Continuity) und der Sicherheit gegenüber Angriffen (Security). Es nutzt die gemäß Architektur vorhandenen Sicherheitselemente und unterbreitet gegebenenfalls Vorschläge für neue Architekturelemente.

Bei einem Rund-um-die-Uhr-Betrieb können beispielsweise duplizierte Rechner zum Einsatz kommen, die als Cluster arbeiten, sowie gespiegelte Platten- und Bändeinheiten. Die duplizierten Komponenten befinden sich hierbei an hinreichend voneinander entfernt gelegenen Standorten. Die Anforderungen an die jeweilige Infrastruktur der Standorte sind ebenfalls festzulegen, wenn sie nicht in Form von Richtlinien, z. B. für Rechenzentren, in standardisierter Form vorlie-

gen. Doch nicht nur auf Ressourcen hat der Rund-um-die-Uhr-Betrieb Auswirkungen, sondern auch auf Prozesse und Organisation, z. B. im Hinblick auf den erforderlichen Schichtbetrieb.

Zum Schutz vor Missbrauch und Angriffen kann ein System beispielsweise mit Verschlüsselungskomponenten für die Übertragung und Speicherung der Daten, mit Firewall, Virenschanner, und Intrusion-Detection-System sowie Chipkarten-Lesegerät oder biometrischem Identifikations- oder Authentifizierungssystem und einem Rechteverwaltungs- und -kontrollsystem mit Protokollierung der Zugänge und Zugriffe ausgestattet sein.

Bei der Spezifikation ist das Prinzip der Konsistenz zu beachten. Dementsprechend spezifiziert der Fachbereich, wie sich die Konsistenz zwischen Eingangsdaten sowie gespeicherten und ausgegebenen Daten prüfen lässt. Dieses Verfahren ermöglicht es, unbeabsichtigte Verarbeitungsfehler sowie Manipulationen zu entdecken.

Die Auswahl des Betriebssystems und seiner Eigenschaften sollte unter Berücksichtigung von Sicherheitsaspekten erfolgen. Hierzu gehört die Betrachtung, welches Sicherheitsniveau das Betriebssystem bietet. Der Schutzmechanismus „Write XOR Execute“, d. h. die Aufteilung von Speicherbereichen in Daten- und Programmbereiche, die entweder beschreibbar oder ausführbar sind, kann eine von verschiedenen Sicherheitseigenschaften eines Betriebssystems sein.

Die Teststrategie legt fest, welche Aspekte bei welchen Testobjekten in welchem Umfang getestet werden sollen. Sie berücksichtigt diesbezügliche unternehmensspezifische Vorgaben, welche die Kritikalitätsklasse mit Testumfang und Testtiefe in Beziehung setzen.

Teststrategie

Auf Basis des Schutzbedarfs und der Sicherheitsklassifizierung wird die Schätzung der Realisierungsdauer- und -kosten verfeinert und den Konsequenzen aus Sicherheitsverletzungen gegenübergestellt. Die Ergebnisse werden mit dem Auftraggeber abgestimmt.

*Verfeinerte
Kosten-
schätzung*

Am Ende des Technischen Grobkonzepts erfolgt ein Sicherheitsreview, in dem überprüft wird, ob die Sicherheitsanforderungen berücksichtigt und angemessen transformiert wurden.

*Sicherheits-
review*

13.5 Technisches Feinkonzept

In der Phase der technischen Feinkonzeption detaillieren die Designer das Grobkonzept weiter bis hin zu Modulspezifikationen und legen die Entwicklungsumgebung fest. Hierbei berücksichtigen sie Sicherheitsaspekte. Diese finden ihren Niederschlag u. a. in folgenden Spezifikationen, Konzepten und Handbüchern:

- Entwicklungsumgebung
- Testspezifikation
- Betriebsführungshandbuch
- Datensicherungskonzept
- Archivierungskonzept
- Notfall- und Katastrophenvorsorgehandbuch.

Entwicklungsumgebung

Für die Entwicklungsumgebung ist z. B. anzugeben, aus welchen Komponenten sie besteht sowie welche Werkzeuge und Programmiersprachen eingesetzt werden. Der Zugang zu Netzen, Systemen und Anwendungen sowie der Zugriff auf Daten sind zu regeln. Es ist zu definieren, welche Anbindungen an welche Netze bestehen und welche Daten zur Verfügung stehen.

Darüber hinaus sind jene Entwicklungsstandards zu referenzieren bzw. erstmalig zu spezifizieren, die bei der Entwicklung eines Informationssystems zu berücksichtigen sind. Hierzu gehören beispielsweise Programmierstandards, die auch sicherheitsrelevante Aspekte im Hinblick auf die eingesetzten Programmiersprachen berücksichtigen.

Plausibilisierung und Konsistenzprüfung

Derartige Standards beinhalten u. a. die Anforderung nach der generellen Schnittstellenplausibilisierung, also der Validierung und Plausibilisierung des Inputs und des Outputs. Bei Web-Anwendungen bezieht sich dies u. a. auf die Plausibilisierung von Request-Parametern, von zurückgelieferten Daten jener Javascript-Programme und Java-Applets, die auf dem Rechner des Benutzers ausgeführt werden, und von ungeschützten Cookies. Außerdem sollten die Standards beschreiben, wie die Integrität und Authentizität von Nachrichten sicherzustellen ist. Verschlüsselung und elektronische Signatur können hierfür in Frage kommen.

Testspezifikation

Testspezifikationen sollten eine unternehmensspezifisch vorgegebene standardisierte Struktur aufweisen, damit alle vorgesehenen Elemente beschrieben werden. Ebenfalls wichtig ist es, den Test bzw. den Abnahmetest als einen Prozess zu sehen, der zu einem frühen Zeitpunkt beginnt und aus unterschiedlichen Schritten besteht [80]. Vor dem eigentlichen Test muss u. a. Folgendes festgelegt bzw. spezifiziert sein:

- der Testplan
- die Teststrategie
- das Testvorgehen

- der spezifische Testumfang und die spezifische Testtiefe, d. h. der Testabdeckungsgrad, je Kritikalitäts- bzw. Sicherheitsklasse
- die Testarten
- die spezifischen Testfelder je Schutzobjektklasse
- die Testumgebung
- die Testszenarien
- die Testfälle einschließlich des Testziels und der erwarteten Ergebnisse
- die Testsequenzen

Die spezifizierten Testfälle decken zum einen den „Schönwetterflug“ ab, der nachweist, dass das System bei ordnungsgemäßer Bedienung das gewünschte Verhalten und die gewünschten Ergebnisse liefert. Bei der Erstellung von Testfällen empfiehlt sich die Bildung von Äquivalenzklassen, z. B. für Daten innerhalb oder außerhalb des Wertebereichs sowie für Grenzwerte. Weitere Aspekte betreffen u. a. die Robustheit gegenüber absichtlichen oder unabsichtlichen Fehlbedienungen sowie fehlerhaften oder unzulässigen Daten, gegenüber Ausnahmesituationen, wie Programm- oder Rechnerabstürzen, und Angriffen.

Das Testvorgehen beschreibt beispielsweise, dass eine Überprüfung der Lieferung sowie ein Installations-, Generierungs- und Konfigurationstest durchgeführt werden. Durch den Generierungstest soll überprüft werden, dass einerseits das System anhand der mitgelieferten Dokumentation generiert werden kann und andererseits das gelieferte ausführbare Programm dem gelieferten Quellcode entspricht.

Testvorgehen

Bei der Testumgebung ist eine Trennung zwischen Entwicklungs-, Test- und Produktionsumgebung sicherzustellen.

Testumgebung

Zu den sicherheitsrelevanten Testarten gehören u. a. Lasttests (Volllast, Langzeit), Performancetests (Antwortzeitverhalten), Kapazitätstest (CPU, Speicher, Kommunikationskanäle, Ein-, Ausgabemedien) sowie Zugangs-, Zugriffs- und Penetrationstests.

Testarten

Organisatorisch ist eine Funktionstrennung zwischen Test- und Entwicklungspersonal vorzusehen.

Testaspekte

Das Betriebsführungshandbuch ist die Grundlage für den späteren Betrieb und damit elementarer Bestandteil der Feinkonzeption. Es enthält die Beschreibung des Informationssystems, Verweise auf die Anforderungen, Übersichts- und Architekturdarstellungen, Beschreibungen der Prozesse und Verweise auf das Datensicherungs- und

Betriebsführungshandbuch

	das Archivierungskonzept sowie das Notfall- und Katastrophenvorsorgehandbuch bzw. den Business Continuity Plan.
<i>Datensicherungskonzept</i>	Das Datensicherungskonzept beschreibt, wann und in welchem Rhythmus welche Daten nach welcher Sicherungsmethode auf welchem Medium an welchem Ort gesichert werden. Hierbei ist die Richtlinie Datensicherung zu berücksichtigen.
<i>Archivierungskonzept</i>	Das Archivierungskonzept legt fest, wann welche Daten auf welchem Medium wo und für welchen Zeitraum archiviert werden sollen. Im Hinblick auf das Thema Sicherheit sind hierbei auch die Anforderungen an das Archiv, z. B. bezüglich Zutrittsschutz, zu spezifizieren.
<i>NuK-Handbuch</i>	Das Notfall- und Katastrophenvorsorgehandbuch wird auf Basis der bereits früher dargestellten Sicherheitsrichtlinie erstellt.

13.6 Entwicklung

<i>Entwicklungsumgebung und Mitarbeiter</i>	Während der Entwicklung ist sicherzustellen, dass die Sicherheit der Entwicklungsumgebung den Sicherheitsanforderungen und der daraus resultierenden Sicherheitsklassifikation entspricht. Dies gilt ebenso für die beteiligten internen und gegebenenfalls externen Mitarbeiter. Neben Vertrauenswürdigkeit müssen die Programmierer über die erforderliche Qualifikation und Erfahrung im Hinblick auf die sichere Entwicklung von Informationssystemen verfügen. Hierzu gehört u. a. die Kenntnis und Umsetzung des Prinzips der Plausibilisierung und der Konsistenz. Durch Nachweise ist zu belegen, dass die Entwickler in unternehmens- und/oder projektspezifischen Entwicklungsstandards und Tools geschult sind und diese Standards einhalten. Außerdem müssen die Programmierer wichtige Angriffsarten, wie z. B. Cross-Site-Scripting, SQL Injection, Command Injection und Buffer-Overflow, und deren Ursachen kennen sowie programmtechnische Schutzmaßnahmen dagegen.
<i>Cross-Site-Scripting (XSS)</i>	Cross-Site-Scripting (XSS) bezeichnet das Einschleusen von Code, z. B. JavaScript®- oder HTML-Code, in eine Webseite. Ursache dieses Angriffsszenarios ist die unzureichende Prüfung, d. h. Plausibilisierung, der zurückgegebenen Eingaben durch eine Webanwendung. Gelingt es einem Angreifer, ausführbaren Code einzuschleusen, so kann er sich hierüber beispielsweise Session-Cookies schicken lassen und Sitzungen des Opfers unter dessen Identität übernehmen. Um dies zu verhindern, sind Prüfungen erforderlich, die ausführbaren Code nicht zulassen, beispielsweise indem Sonderzeichen durch Escape-Sequenzen ersetzt werden.

Beim Einsatz von SQL-Abfragen ist sicherzustellen, dass die zurückgelieferten Parameter keine Manipulationsmöglichkeiten des SQL-Befehls durch SQL-Injektion eröffnen. Dementsprechend sind die Daten zu plausibilisieren, also u. a. zu prüfen auf

SQL-Injektion

- SQL String Delimiter (‘),
- SQL Statement Concatenation Character (;) und
- SQL Comment Sequence bzw. Character (bei Microsoft® SQL Server: –, bei MySQL: #).

Sind derartige Zeichen in der Zeichenkette eines Parameters zulässig, so ist sicherzustellen, dass das Programm diese Zeichen als Bestandteil der Zeichenkette und nicht des SQL-Befehls interpretiert. Dies kann oftmals durch Voranstellen eines Backslash „\“ erfolgen.

Bei der Programmierung, insbesondere auch in C und C++, sind die Risiken durch Pointer und Pufferüberläufe, d. h. Buffer-Overflows, zu berücksichtigen. Die Ursache des Pufferüberlaufs liegt auch hier in einer fehlenden Plausibilisierung. Ein Programm kopiert in diesem Fall Daten, z. B. Eingabedaten, in einen Speicherbereich fester Größe, ohne zuvor die Größe dieser Daten zu prüfen. Ist die Datenmenge zu groß, so kommt es zu einem Überlauf des Speicherbereichs. Die überzähligen Daten überschreiben den an den Puffer angrenzenden Speicherbereich und damit die dortigen Daten. Dies kann zu einem Absturz des Programms führen oder dazu, dass beim Rücksprung aus einem Unterprogramm auf einen Speicherbereich gesprungen wird, in dem sich der mit den Eingabedaten mit eingeschleuste Schadcode befindet.

*Pufferüberläufe,
Buffer Overflow*

In der Programmiersprache C kann die falsche Verwendung der Funktionen *strcpy* und *strcat* zu derartigen Problemen führen. Die Funktionen *memcpy*, *strncpy* bzw. *strncat* gemäß ANSI X3.159-1989, besser noch *strncpy* und *strlcat* aus OpenBSD 2.4, berücksichtigen die mit übergebene Länge. Problematisch ist auch die Ausgabe von Zeichen in ein character array mittels *sprintf*. Demgegenüber berücksichtigt *snprintf* die vorgegebene Maximallänge der Zeichenkette.

Die Konfiguration der Entwicklungsumgebung und der entwickelten Module, Komponenten und Systeme muss das Konfigurationsmanagement nachvollziehbar halten und manipulationssicher gestalten.

Konfiguration

Der Zugriff auf den Source-Code ist über geeignete Maßnahmen zu schützen. Änderungen sind unter Berücksichtigung des Change-Request-Verfahrens durchzuführen.

<i>Code-Inspektionen und Walkthroughs</i>	Während der Programmentwicklung führen Prüfer Code-Inspektionen und gemeinsam mit den Entwicklern Code-Walkthroughs durch, je nach Sicherheitsanforderung auch nur stichprobenartig. Hierbei prüfen sie den der Quellcode z. B. auf unzulässige Code-Passagen und die Einhaltung der Entwicklungsstandards. Jeder Entwickler testet die von ihm entwickelten Module ferner auch hinsichtlich der definierten Sicherheitskriterien und stellt sie erst nach erfolgreichem Test für die Integration zur Verfügung.
<i>Externe Entwicklung</i>	Soll ein Dienstleister die Entwicklung durchführen, so ist er, wie jedes Outsourcing-Unternehmen, im Vorfeld zu prüfen. Hierbei ist sicherzustellen, dass der Entwicklungsprozess angemessen ist, er Sicherheitsaspekte berücksichtigt sowie die Anforderungen und Entwicklungsstandards des Auftraggebers erfüllt. Ein geeignetes Projektmanagement ist erforderlich.

13.7 Integrations- und Systemtest

<i>Prämissen</i>	Für den Integrations- und Systemtest ist eine Trennung von Entwicklungs-, Test- und Produktionsumgebung sicherzustellen. Sollten Datenbestände aus der Produktionsumgebung genutzt werden, so sind diese vorher zu pseudonymisieren. Ferner muss eine Funktions-trennung zwischen Test und Entwicklung hergestellt werden.
<i>Testumfang</i>	Die sicherheitstechnische Überprüfung der ausführbaren Programme erfolgt durch Tests. Eine minimale Anforderung ist z. B., dass die Test-Funktionsmatrix an jedem Kreuzungspunkt mindestens einen Test nachweist. Je höher die Sicherheitsanforderungen an ein System sind, desto umfangreichere Tests müssen z. B. hinsichtlich Sicherheit, Kontinuität, Stress, Last, Performance, Testabdeckungsgrad etc. durchgeführt werden. Webanwendungen sollten Tester insbesondere auch auf bekannte Schwachstellen hin untersuchen, wie z. B. Cross-Site-Scripting, SQL-Injektion und Buffer-Overflow. Zur Steigerung der Effizienz ist die Nutzung verfügbarer Tools anzuraten [81].
<i>Integrationstest</i>	Beim Integrationstest werden Module zu Komponenten zusammengefügt und diese getestet.
<i>Systemtest</i>	In der Phase des Systemtests erfolgt der Test des Gesamtsystems. Zu Beginn sollte dabei geprüft werden, dass alle Testobjekte vorhanden sind. Dies betrifft beispielsweise die Dokumentation, die vom Quellcode über das Benutzer-, Installations-, Customizing- und Generierungshandbuch bis zum Betriebsführungshandbuch reichen kann.
<i>Nachvollziehbarkeit</i>	Die Tester müssen die durchgeführten Tests nachvollziehbar dokumentieren. Dies beinhaltet die Angabe der Systemkonfiguration mit

den Releaseständen der einzelnen Systemkomponenten, den genutzten Datenbestand und die durchgeführten Tests samt Testergebnis sowie die Angabe des Testdatums und des Testers.

13.8 Freigabe

Nach (hinreichend) erfolgreichem Abschluss des Systemtests erfolgt die Freigabe des Systems. Diese wird in Form einer Freigabebestätigung, gegebenenfalls mit noch zu behebenden Problemen, deren Schweregrad und Zielterminen, dokumentiert.

13.9 Software-Evaluation

Anstelle der bisher beschriebenen unternehmensinternen Software-Entwicklung können die Verantwortlichen nach der Fachspezifikation entscheiden, das Informationssystem entweder fertig zu kaufen oder extern entwickeln zu lassen.

Möchte der Fachbereich ein Standardprodukt kaufen, so erfolgt anstelle der Entwicklung die Evaluation der am Markt angebotenen Informationssysteme. Die Evaluatoren stellen hierzu z. B. funktionale, sicherheitstechnische und finanzielle Kriterien auf und gewichten diese. In diesem Zusammenhang bewerten und auditieren sie den potenziellen Auftragnehmer hinsichtlich seines Sicherheitsniveaus, etablierter und eingehaltener Standards, vorhandener Zertifizierungen, seiner finanziellen Stärke und Stabilität sowie der Referenzen und eventuellen Abhängigkeiten bzw. Zugehörigkeiten zu Unternehmensgruppen, z. B. von Mitbewerbern oder Herstellern. Je nach Erfahrung des Unternehmens kann es sich hierbei auch von einer geeigneten Unternehmensberatung unterstützen lassen.

*Standard-
produkt*

Bei externer Entwicklung regeln Auftraggeber und -nehmer verschiedene sicherheitsrelevante Aspekte vertraglich (s. a. [6]): Hierzu gehören die rechtlichen Verhältnisse bezüglich Geheimhaltung, Copyright und Source-Code sowie gegebenenfalls lizenzrechtliche Thematiken. Auftraggeber und -nehmer vereinbaren außerdem sicherheitsrelevante externe und auftraggeberinterne Standards und Vorgaben, die zu beachten sind, sowie Kontrollmöglichkeiten des Auftraggebers während der Entwicklung. Sicherheits-, Qualitäts- und Abnahmekriterien sowie Fehlerklassen sind ebenfalls Gegenstand der Vereinbarung, die sich üblicherweise aus dem Fachkonzept sowie unternehmensinternen Standards ergeben. Das Thema Know-how-Transfer ist ein wesentliches Vertragselement. Ein geeignetes Projektmanagement ist aufzustellen, zu verabschieden und vertraglich

zu fixieren. In ihm adressieren die Beteiligten auch sicherheitsrelevante Themen. Häufigkeit und Inhalt des Berichtswesens sind ebenso wie Jour fixes festzulegen.

Nach der Beauftragung der Software-Entwicklung oder dem Kauf einer Software ist der Einsatz eines Treuhänders, z. B. einer Escrow-Agentur, zu erwägen. Sie verwaltet den Quellcode als Zwischeninstanz treuhänderisch bis zu einem vordefinierten Ereignis, z. B. der Insolvenz des Auftragnehmers.

*Externe
Entwicklung*

Eine Bewertung sollte auch bei der Vergabe von Entwicklungsaufträgen an einen externen Dienstleister vorgenommen werden.

13.10 Auslieferung

Das freigegebene ITK-System liefert der Auftragnehmer an den internen oder externen Kunden. Im Hinblick auf den Lieferweg ist sicherzustellen, dass keine Veränderungen (Manipulationen) stattfinden können sowie Einsichtnahme und Verlust ausgeschlossen sind. Diesbezügliche Sicherheitsmaßnahmen bestehen beispielsweise in einer Empfangsbestätigung sowie Verschlüsselung und digitaler Signatur.

13.11 Abnahmetest und Abnahme

*Abnahme-
prozess*

Der Abnahmeprozess, beginnend bei der Entwicklung des Abnahmehandbuchs, ist in [80] überblicksartig beschrieben. Bei der Entwicklung der Testfälle ist darauf zu achten, dass die vielfältigen externen Anforderungen, u. a. aus dem HGB oder aus den Grundsätzen für eine ordnungsmäßige Datenverarbeitung berücksichtigt werden.

Generierung

Der Auftraggeber, z. B. die auftraggebende Abteilung in einem Unternehmen, unterzieht das bereitgestellte ITK-System dem Abnahmetest. Insbesondere bei der Lieferung durch einen externen Auftragnehmer ist anhand einer Liste sicherzustellen, dass die Lieferung vollständig ist [80]. Im Hinblick auf Sicherheit ist zu prüfen, dass der Quellcode mit dem ausführbaren Programm übereinstimmt. Dies erfordert nach dem Einspielen des Quellcodes die Generierung des ITK-Systems [6]. Hiermit prüfen die Tester gleichzeitig, ob die Generierung möglich ist und das Generierungshandbuch den hierfür erforderlichen Ablauf korrekt und verständlich beschreibt.

*Test der
Sicherheits-
anforderungen*

Im Rahmen der Abnahme ist insbesondere auch die Umsetzung der Sicherheitsanforderungen zu testen. Dies betrifft beispielsweise die Umsetzung der Zugangs- und Zugriffskonzepte sowie der Last-,

Performance- und Verfügbarkeitsanforderungen sowie den Schutz vor Angriffen.

Im Anschluss an die vordefinierten Testfälle sollte der Abnahmeprozess eine Phase freien Testens vorsehen, in der erfahrene und fachlich versierte Tester intuitiv testen.

Freies Testen

Die durchgeführten Tests sind in einem Testprotokoll nachvollziehbar zu dokumentieren. Nach erfolgreichem Abschluss der Abnahme erstellt der Testmanager ein Abnahmeprotokoll mit gegebenenfalls noch vorhandenen Mängeln, Behebungszeitpunkten und Konsequenzen bei Nichterfüllung. Das Abnahmeprotokoll gibt ferner an, welchen Schweregrad der aufgetretene Fehler besitzt und in welchem Umfang ein Nachtest vorgesehen ist. Je nach Testmöglichkeiten empfiehlt es sich, die Inbetriebnahme mit Parallelbetrieb und/oder Pilotierung, als Teil der Abnahme vorzusehen.

*Test- und
Abnahme-
protokoll*

Praxistipp

Die Ersteller von Testfällen sollten diese in einer Testfalldatenbank in standardisierter Form dokumentieren. Hierbei sollte erkennbar sein, welche Testfälle welche Funktionalitäten oder Eigenschaften, z. B. Robustheit, Ausfallsicherheit, Angriffssicherheit oder Leistungsfähigkeit testen. So lassen sich Auswertungen darüber erstellen, in welchem Umfang welche Bereiche des ITK-Systems zu testen sind.

Die Datenbank sollte ferner so gestaltet sein, dass sich auch die Ergebnisse festhalten lassen. Auf diese Weise kann der Testmanager durch entsprechende Auswertungen und Statistiken während des Abnahmetests nachverfolgen und darüber berichten, wie der Abnahmetest vorankommt, an welchen Stellen Probleme auftauchen, bis wann diese behoben sind etc.

Hinsichtlich Effizienz und Standardisierung sollte eine Testfalldatenbank als Hilfsmittel unternehmensweit zur Verfügung stehen.



*Testfall-
datenbank*

13.12 Software-Verteilung

Ist eine Software-Verteilung erforderlich, so muss sichergestellt werden, dass hierbei die Sicherheitsanforderungen berücksichtigt werden. Bei der Übertragung oder dem Transport sind den Anforderungen entsprechend Maßnahmen gegen eine Manipulation, Löschung, Einsichtnahme oder Entwendung vorzusehen.

13.13 Inbetriebnahme

*Inbetriebnahme,
Parallelbetrieb
und
Pilotierung*

Die Inbetriebnahme kann auf einen Schlag und damit in der Regel risikoreich in Form eines „Big Bang“ erfolgen, oder in einzelnen Schritten. In der Phase des Parallelbetriebs betreibt der Auftraggeber das neue ITK-System über einen angemessenen Zeitraum parallel zu einem bestehenden ITK-System. Deren Ergebnisse vergleicht er. Hierbei verifiziert er außerdem, dass die Prozesse, Ressourcen und die Organisation die gestellten Anforderungen erfüllen. In der Pilotierungsphase führt der Auftraggeber das ITK-System in einem repräsentativen aber begrenzten Umfeld ein und testet es im operativen Betrieb. Die Ergebnisse dieser Phasen sollten abnahmerelevant sein.

13.14 Betrieb

Während der Betriebsphase des ITK-Systems muss der Bereich Informationsservices Probleme und Änderungen in den ITK-Systemen nachvollziehbar dokumentieren und aufbewahren. Dies betrifft auch die Dokumentation der Zutritts-, Zugangs- und Zugriffsberechtigungen sowie Protokolldateien.

Der Bereich Informationsservices gestaltet den Betrieb mit allen im Kapitel Sicherheitsarchitektur beschriebenen Ressourcen und ITK-Prozessen. Wesentliche Prozesse sind der dort beschriebene ITK-Betriebsprozess samt Begleitprozessen (Managementdisziplinen). Der Bereich Informationsservices betreibt die Anwendungen und Systeme gemäß den dokumentierten Betriebsführungshandbüchern. Er hält die definierten Richtlinien und Konzepte ein und setzt die geforderten Maßnahmen um.

*Monitoring,
Controlling,
Reporting*

Die Überwachung, d. h. das Monitoring, der ITK-Ressourcen und -Prozesse im Hinblick auf sicherheitsrelevante Ereignisse ist ein wesentliches Element des ITK-Betriebs. Zu derartigen Ereignissen gehören z. B. Störungen, Ausfälle und Angriffe. Hinzu kommen das Sicherheits-Controlling und das Berichtswesen (Safety-Security-Reporting). Informationen zu den Inhalten finden Sie im Kapitel Sicherheitsregelkreis.

*Computer
Security
Incident
Management*

Im Rahmen des Sicherheitsmanagements legt z. B. der Bereich Informationsservices für die Behandlung sicherheitsrelevanter Ereignisse (security incident) die Beteiligten, deren Alarmierung und die Vorgehensweise fest. Er baut hierfür ein Information Security Incident Management auf. Je nach Unternehmensorganisation übernimmt ein Computer Security Incident Response Team (CSIRT) die weitere Behandlung des Ereignisses. Für Notfälle im Hinblick auf die Ge-

schäftskontinuität sind ebenfalls die Beteiligten, z. B. Notfallbeauftragte und Notfallteams, deren Alarmierung und die Vorgehensweise festzulegen.

Will ein Unternehmen den Betrieb an ein Outsourcing-Unternehmen auslagern, so prüft es dieses im Vorfeld auch unter Sicherheitsaspekten (s. a. „Handbuch Unternehmenssicherheit“ des Autors). Im Vertrag sind auch die sicherheitsrelevanten Anforderungen zu vereinbaren. Hierzu kann beispielsweise gehören, dass

Outsourcing

- die buchungsrelevanten Systeme bei einem Ausfall spätestens nach 24 Stunden alle buchungstechnisch relevanten Daten vollständig, richtig und für einen sachverständigen Dritten nachvollziehbar und GoB-entsprechend wieder bereitstellen
- die Systeme ein bestimmtes Sicherheitsniveau erreichen müssen, z. B. F-C2 der früheren ITSEC oder bestimmte Klassen der ISO/IEC 15408:1999
- die Ordnungsmäßigkeit der Dienstleistung sichergestellt ist
- der Auftraggeber die erforderlichen Kontrollmöglichkeiten erhält
- der Auftragnehmer dem Auftraggeber die erforderlichen Weisungsbefugnisse einräumt
- der Aufsichtsbehörde, z. B. der BaFin, entsprechende Prüfungs- und Kontrollmöglichkeiten eingeräumt sind.

13.15 Außerbetriebnahme

Bei der Außerbetriebnahme von ITK-System dokumentiert der Bereich Informationsservices, wer welche Komponenten in welchem Releasestand wann außer Betrieb nimmt. Er legt ebenfalls dar, ob und wenn ja wie jemand die verschiedenen Komponenten von Hard- über Software und Daten bis hin zu Dokumentation weinternutzt, migriert, archiviert oder unter Berücksichtigung der Vertraulichkeit vernichtet. Diese Informationen dokumentiert der Bereich Informationsservices nachvollziehbar im Außerbetriebnahmeprotokoll.

*Außerbetrieb-
nahmeprotokoll*

Für die Ewigkeit bestimmt?

Im Serverraum eines Unternehmens befanden sich mehrere ITK-Systeme. Eine Überprüfung der Systeme ergab, dass eins der System zwar noch betrieben, aber nicht mehr genutzt wurde.



Unter Sicherheitsaspekten müssen die Verantwortlichen ferner berücksichtigen, wie lange die Daten aufzubewahren und ihre Lesbarkeit sicherzustellen sind. Als Konsequenz kann sich hieraus ergeben,

*Weitere
Sicherheits-
aspekte*

dass sie zusätzlich Hard-, Soft-, Paper- und Processware archivieren und verfügbar halten müssen. Gegebenenfalls kann gleich oder während der Aufbewahrungsfrist die Migration von Datenbeständen, die Prüfung der Lesbarkeit und das regelmäßige Überspielen auf neue Datenträger erforderlich werden.

13.16 Hilfsmittel Phasen-Ergebnistypen-Tabelle

*Phasen-
Ergebnistypen-
Tabelle*

Mittels einer Tabelle können IT-Sicherheitsbeauftragte die sicherheitsrelevanten Ergebnistypen der einzelnen Phasen im Prozess- bzw. Systemlebenszyklus darstellen. Für jeden Ergebnistyp sollte es eine Vorlage mit Struktur und Inhalten sowie bei Bedarf eine Vorgehensweise geben. Es empfiehlt sich, diese Phasen-Ergebnistypen-Tabelle im Intranet so bereit zu stellen, dass der Nutzer von den genannten Phasen und Ergebnistypen über entsprechende Links direkt zu den dazugehörigen Inhalten, Vorlagen und Vorgehensweisen gelangen kann.

*Qualitäts-
sicherung*

Für jeden Ergebnistyp sollte angegeben werden, wie seine Qualitätssicherung erfolgt. Bei Konzepten empfiehlt sich beispielsweise die Durchführung eines Reviews (R). Entsprechende spezifische Hilfsmittel in Form von Prüflisten und Prüfkriterien sollten zur Verfügung gestellt und über einen Link angebunden werden.

Erforderlichkeit

Ebenfalls sollte angegeben werden, ob der jeweilige Ergebnistyp zwingend (z) oder optional (o) bzw. bei welcher Verfügbarkeits-/Sicherheitsklasse erforderlich ist

Checkliste

Die folgende auszugsweise Phasen-Ergebnistypen-Tabelle kann der Projektleiter gleichzeitig als Checkliste verwenden, um die Vollständigkeit der Ergebnistypen je Phase sicherzustellen. Dies lässt sich in der Spalte Status (z. B. gestartet (s), beendet (e), geprüft/getestet (t), freigegeben (f)) eintragen.

Phase		Status		
Ergebnistyp		QS-Methode		
Teilergebnisse		Zwingend/optional		
Beantragung				
...				
Fachkonzeption				
Schutzbedarfsanalyse		Z	R	
Klassifizierung		Z	R	
Zugangsberechtigungskonzept		Z	R	
Zugriffsberechtigungskonzept		Z	R	
Datensicherungsanforderungen		Z	R	
Archivierungsanforderungen		Z	R	
...				
...				
Technische Grobkonzeption				
Verifizierte Schutzbedarfsanalyse		Z	R	
...				
...				
Technische Feinkonzeption				
Datensicherungskonzept		Z	R	
Archivierungskonzept		Z	R	
Notfall- und Katastrophenvorsorgehandbuch		Z	R	
Testhandbuch		Z	R	
...				
...				
...				

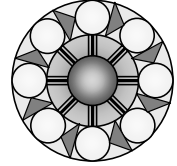
13.17 Zusammenfassung

Das Sicherheits-, Kontinuitäts- und Risikomanagement sollte prozess-, ressourcen-, produkt-, dienstleistungs- und lebenszyklusimmanent gestaltet sein. Dies erfordert eine erste Betrachtung der Sicherheitsanforderungen bei der Beantragung und Wirtschaftlichkeitsprüfung eines ITK-Systems. Die Sicherheitsanforderungen sind – unabhängig vom zugrunde gelegten Phasen- oder Entwicklungsmodell – phasenweise weiter zu verfeinern und zu prüfen.

<i>Fachkonzept, technisches Konzept</i>	Während der Fachkonzeption erfolgt die Erhebung des Schutzbedarfs und die Sicherheitsklassifizierung des ITK-Systems. Designer transformieren die fachlichen Anforderungen für das technische Grob- bzw. Feinkonzept in technische Anforderungen. Im Grobkonzept legen sie außerdem die Teststrategie fest.
<i>Technisches Feinkonzept</i>	In der Phase des technischen Feinkonzepts entstehen über die Modulspezifikationen hinaus z. B. die Testspezifikation, das Betriebsführungshandbuch, das Datensicherungs- und das Archivierungskonzept sowie das Notfall- und Katastrophenvorsorgehandbuch bzw. der Business Continuity Plan.
<i>Entwicklung</i>	Bei der Auswahl der Entwicklungsumgebung, der beteiligten Personen und der Prüfverfahren berücksichtigt das Entwicklungsteam die Sicherheitsanforderungen. Beim Kauf von Standardsoftware oder der Vergabe des Software-Entwicklungsauftrags an Dritte sind verschiedene zuvor genannte Sicherheitsaspekte und Kontrollmöglichkeiten vertraglich und entwicklungsbegleitend zu berücksichtigen.
<i>Test</i>	Testumfang, Testarten und Detaillierungsgrad orientieren sich an den Sicherheitsanforderungen. Der Abnahmetest sollte Generierungs- und Installationstests sowie Zugangs-, Zugriffs- Last-, Performance- und Verfügbarkeitstests umfassen. Freies Testen, Parallelbetrieb und Pilotierung sind abhängig von den Sicherheitsanforderungen durchzuführen. Der Umfang und das Ergebnis der Abnahme müssen nachvollziehbar protokolliert werden.
<i>Betrieb, Outsourcing</i>	Im Betrieb der ITK-Systeme muss der Bereich Informationsservices die Einhaltung der Sicherheitsanforderungen erreichen und überprüfen. Beim Outsourcing müssen die Sicherheitsanforderungen mit dem Outsourcer vereinbart werden.
<i>Außerbetriebnahme</i>	Die Außerbetriebnahme sollte als eigene Phase berücksichtigt sein. Sicherheitsanforderungen sind zu berücksichtigen und die Außerbetriebnahme ist angemessen zu protokollieren.
<i>Prozesse</i>	In allen Phasen des Lebenszyklus müssen die jeweiligen Verbindungsstellen zu den Prozessen und Ressourcen berücksichtigt und bedient werden.

14 Sicherheitsregelkreis

Alles fließt (παντα ρει, Heraklit), d. h. alles verändert sich: Bedrohungen, Angriffsmöglichkeiten, Schutzbedarf, Prozesse, Ressourcen, Technologie, Organisation und last, but not least, das Personal. Dementsprechend unterliegen alle Elemente der Sicherheitspyramide einer kontinuierlichen Anpassung, Veränderung und Weiterentwicklung.



Wie können diese Veränderungen und der Status des Sicherheits- und Kontinuitätsmanagements, oder – umgekehrt formuliert – des Risikomanagements, ermittelt werden? Erinnern wir uns an den detaillierten Risikodreiklang des Autors, so setzt sich das Risiko aus dem Schadens-, Bedrohungs- und Schwachstellenpotenzial zusammen. Diese lassen sich im Rahmen einer Sicherheitsprüfung bzw. Risikoanalyse erheben und zeigen – quasi als Momentaufnahme – den Status des Risiko- bzw. Sicherheitsmanagements. Sicherheitslücken werden so erkennbar und können gestopft werden.

Derartige „Schnappschüsse“ werden jedoch der kontinuierlichen Veränderung des Umfelds nicht ausreichend gerecht. Daher muss der Chief Information Security Officer (CISO) das Sicherheitsmanagement zusätzlich kontinuierlich steuern und nachvollziehbar gestalten. Hierbei spielen die Perspektiven Finanzen, Kunden, Prozesse sowie Lernen und Entwicklung, wie sie aus der Balanced Scorecard (BSC) [11] bekannt sind, eine wesentliche Rolle. Die IT-Sicherheits-BSC (ISi-BSC) des Autors zusammen mit dem Controlling-Regelkreis liefern das „Handwerkszeug“ hierzu. Diese Themen sind in den folgenden Unterkapiteln beschrieben:

1. Sicherheitsprüfungen
2. Sicherheitscontrolling
3. Berichtswesen (Safety-Security-Reporting)
4. Safety-Security-Benchmarks
5. Hilfsmittel IT-Sicherheitsfragen
6. Zusammenfassung

14.1 Sicherheitsprüfungen

Alles sicher, oder nicht?

(Dr.-Ing. Klaus-Rainer Müller, 11. Februar 2005)

Die Prüfungen im Sicherheits- und Kontinuitätsmanagement dienen dazu, festzustellen, ob das gewünschte Sicherheits- und Kontinuitätsniveau erreicht worden ist. Diese Prüfungen haben je nach ihrem Fokus und Umfang unterschiedliche Bezeichnungen wie z. B. Scans, Sicherheitschecks, Sicherheitsaudits, Gap-Analysen, Sicherheitsstudien, Risikoanalysen oder auch Penetrationstests.

Sowohl Prüfer als auch Geprüfte sollten diese Aussage beherzigen:

Fehler zu finden ist leichter, als keine zu machen!

(Dr.-Ing. Klaus-Rainer Müller, 8. November 2006)

14.1.1 Sicherheitsstudie/Risikoanalyse

Das prinzipielle Vorgehen bei Sicherheitsstudien bzw. Risikoanalysen ist in der folgenden Abbildung dargestellt.

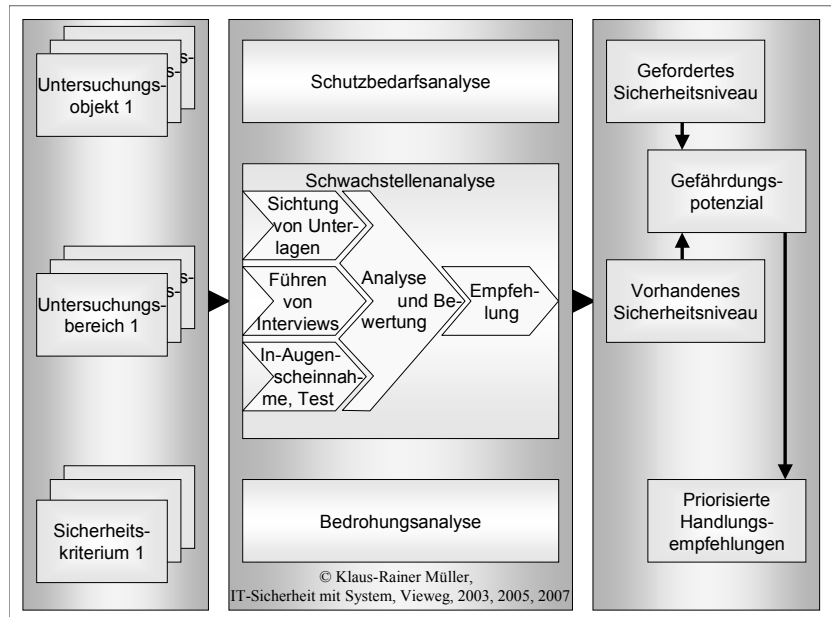


Abb. 14.1: Sicherheitsstudie/Risikoanalyse

Eine Sicherheitsstudie unterteilt sich in folgende Phasen:

1. Definition des Untersuchungsumfangs und der Rahmenbedingungen
2. Durchführung der Erhebung, Analyse und Bewertung sowie Ermittlung des Deltas zwischen Soll und Ist
3. Entwicklung von Handlungsempfehlungen.

Um den Untersuchungsumfang festzulegen, ist die folgende Frage zu beantworten: Was ist woraufhin in welchem Detaillierungsgrad bis wann von wem in welcher Art mit welchen Hilfsmitteln (z. B. Fragenkataloge/Checklisten, Security-Scanner) zu untersuchen.

*Unter-
suchungs-
umfang*

Zuerst legen Auftraggeber und Auftragnehmer das „was“ fest, d. h. die Untersuchungsobjekte. Dies sind z. B. Informationssysteme, Hardwareplattformen und Infrastruktur. Das „woraufhin“ unterteilt sich in die Untersuchungsbereiche und die Sicherheitskriterien, die betrachtet werden sollen. Untersuchungsbereiche sind beispielsweise die Prozesse, Ressourcen und Organisation, Sicherheitskriterien, z. B. die Verfügbarkeit, die Vertraulichkeit und die Integrität.

Die Festlegung des Detaillierungsgrads ist mitbestimmend für den Aufwand und die Dauer der Untersuchung. Von wem die Untersuchung durchgeführt werden soll, ist abhängig davon, ob z. B. spezielle Expertisen, Neutralität und unternehmensübergreifendes Wissen oder auch personelle Zusatzkapazität gefragt sind. Dementsprechend kommen externe Berater, die Revision oder der IT-Sicherheitsverantwortliche des Unternehmens in Betracht.

*Detaillierungs-
grad*

Im Hinblick auf die Art der Untersuchung legen Auftraggeber und -nehmer fest, welche Dokumente der Auftraggeber zur Verfügung stellt und ob der Auftragnehmer Interviews, Begehungen und Tests durchführen soll. Ebenfalls im Vorfeld sollten beide Seiten abstimmen, ob es Einschränkungen oder Vorgaben bei den eingesetzten Hilfsmitteln, z. B. Security-Scanner zu beachten gilt.

*Unter-
suchungsart*

Die Durchführung der Erhebung, Analyse und Bewertung untergliedert sich gemäß der Definition des „Risikos“ im Risikodreiklang des Autors in folgende drei Teilbereiche:

Durchführung

1. Schutzbedarfsanalyse
2. Schwachstellenanalyse
3. Bedrohungsanalyse

<i>Schutzbedarfs-, Schwachstellen-, Bedrohungsanalyse</i>	Die Schutzbedarfsanalyse wurde bereits im Kapitel Sicherheitsziele erläutert. Die Schwachstellenanalyse beinhaltet die Sichtung der bereitgestellten Unterlagen, die Durchführung von Interviews und/oder Workshops sowie je nach Umfang die Begehung bzw. Inaugenscheinnahme und den Test. In der Bedrohungsanalyse werden potenzielle Bedrohungen erhoben, die sich z. B. aus dem Standort des Unternehmens, seiner Marktposition, seinem Image, seiner aktuellen Situation oder dem technologischen, wirtschaftlichen und politischen Umfeld ergeben.
<i>Sicherheitsniveau</i>	Die Ergebnisse dieser drei Analysen, die jeweils die Erhebung, Analyse und Bewertung beinhalten, liefern das geforderte und das vorhandene Sicherheitsniveau. Der Soll-Ist-Vergleich ergibt eine Differenz, die für die Priorisierung der Handlungsempfehlungen wichtig ist.
<i>Momentaufnahme</i>	Da Sicherheitsstudien naturgemäß begrenzt sind und eine Momentaufnahme bzw. einen „Schnappschuss“ (snapshot) darstellen, sollten sie in regelmäßigen Abständen nach einem vordefinierten Zeitplan durchgeführt werden.
<i>HAZOP</i>	Die Hazard and Operability Analysis (HAZOP), d. h. die Gefahren- und Betriebsfähigkeitsanalyse, ist eine qualitative formale Methode, um das Verhalten von Anlagen und Systemen sowie Prozessen bei unterschiedlichen Fehlern zu ermitteln sowie Maßnahmen zu deren Absicherung zu ergreifen. Ursprünglich hat die chemische Industrie die HAZOP entwickelt und eingesetzt. Später wurde HAZOP zur Anwendung bei Software erweitert.
<i>HAZOP-Leitwörter</i>	Eine HAZOP wird in kreativen interdisziplinären Teams durchgeführt, die über tiefgehendes Wissen um das Untersuchungsobjekt verfügen. Anhand von Leitwörtern, wie z. B. kein, mehr, weniger, teilweise, andere, entgegengesetzt/verkehrt herum, gleichzeitig, früher als, später als, postulieren die Mitwirkenden hypothetische Abweichungen vom regulären Verhalten. Das HAZOP-Team erstellt anhand der Leitwörter in einem ersten Schritt Matrizen. Diese stellen den Elementen und Eigenschaften des Untersuchungsobjekts die Leitwörter gegenüber. In die Matrizenfelder trägt das Team deren Anwendbarkeit ein.

Leitwort Element	kein	mehr	weniger	teilweise	andere	...
Spannung	Keine	Über- spannung	Unter- spannung	Schwankung	N/A	...
Klimatisierung	Keine	Zu kalt	Zu warm	Schwankung	N/A	...
...	...	...	...	...	...	...

Für jedes hypothetische Ereignis ermittelt das Team Abweichungen und mögliche Ursachen. Hieraus leitet es Folgen ab und beschreibt Möglichkeiten zur Erkennung und Empfehlungen oder zu klärende Punkte.

Wer Verantwortung trägt für Ressourcen, z. B. Anlagen und ITK-Systemen, oder Prozesse sollte HAZOPs während des Lebenszyklus und bereits in der Designphase durchführen. Basis derartiger Analysen sind beispielsweise Gebäude-, Anlagen- und Schaltpläne. Bei Software-Systemen nutzen HAZOPs Netztopologie, Anwendungsarchitekturen, Blockdiagramme, Datenflussdiagramme, objektorientierte Designdiagramme, wie Strukturdiagramme, z. B. Klassen-, Komponenten- und Kompositionsstrukturdiagramme, und Verhaltensdiagramme, z. B. Aktivitäten-, Anwendungsfall- (use cases), Kommunikations- und Zustandsdiagramme.

Ein spezielles Vorgehen zur Risikoanalyse für Informationssysteme beschreibt der OCTAVE® approach [82], den das Software Engineering Institute (SEI) der Carnegie Mellon University entwickelt hat. OCTAVE® steht für Operationally Critical Threat, Asset and Vulnerability Evaluation. Eine derartige Risikoanalyse betrachtet die drei Komponenten des Risikos (s. Risikodreiklang), d. h. Bedrohungen, Werte und Schwachstellen. Das Vorgehen unterteilt sich in drei Phasen mit insgesamt acht Prozessen. Diese Methode ist anwendbar auf große Unternehmen (z. B. mehr als 300 Mitarbeiter) sowie als OCTAVE®-S für kleine Organisationen.

*IT-Risikoana-
lyse mit
OCTAVE®*

In der Phase 1, die aus 4 Prozessen besteht, erstellt das Analyse-Team die Bedrohungsprofile der informationsbezogenen Werte. Es ermittelt zuerst die wichtigen informationsbezogenen Werte und die derzeitigen Schutzmaßnahmen. Diese Informationen erhebt es beim Senior Management (Prozess 1), bei den Managern der operativen Ebene (Prozess 2) und bei den Mitarbeitern (Prozess 3). Dann wählt es kritische Werte (assets) aus und beschreibt deren Sicherheitsanforderungen (Schutzbedarf). Schließlich identifiziert es die jeweiligen Bedrohungen und erstellt für jeden Wert ein Bedrohungsprofil (Prozess 4).

Phase 1

In der Phase 2 erhebt das Analyse-Team die Schwachstellen der Infrastruktur. Hierzu identifiziert es einen repräsentativen Satz von IT-Komponenten, die den kritischen Werten zugeordnet sind, und definiert ein Vorgehen zu deren Bewertung (Prozess 5). Dann ermittelt das Team, wie widerstandsfähig jede Komponentenkategorie ist (Prozess 6).

Phase 2

In der dritten und letzten Phase identifiziert das Analyse-Team die Risiken der kritischen Werte (Prozess 7) und entwickelt eine Schutz-

Phase 3

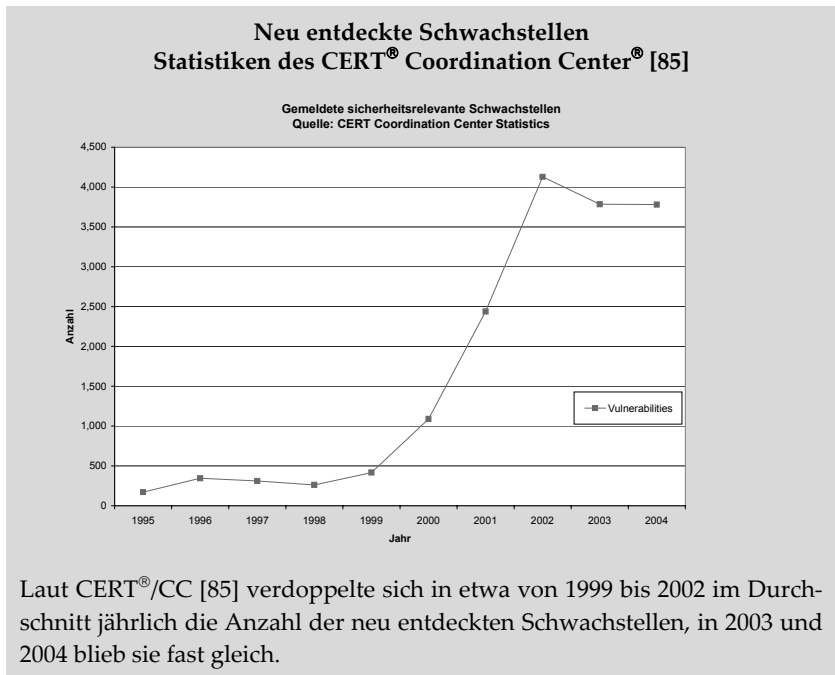
strategie zur Risikoreduzierung (Prozess 8). Bei der Ermittlung des Risikos werden Eintrittswahrscheinlichkeiten derzeit nicht berücksichtigt, können aber eingefügt werden. Zukünftige Überarbeitungen der OCTAVE®-Methode enthalten voraussichtlich optional qualitative Schätzungen der Eintrittswahrscheinlichkeit. Weiterführende Informationen finden Sie in [83].

Security Self-Assessment von IT-Systemen gemäß NIST

Das NIST hat einen Security Self-Assessment Guide for Information Technology Systems entwickelt [84]. Er dient dazu, den aktuellen Status der Informationssicherheit festzustellen und – sofern notwendig – Ziele für Verbesserungen aufzuzeigen. Zur Feststellung des Status dient ein Fragenkatalog.

14.1.2 Penetrationstests

Mit Penetrationstests wird versucht, in unbefugter Weise, d. h. ohne entsprechende Berechtigungen, in Kommunikationsnetze und Informationssysteme einzudringen.



Die Statistik zeigt, dass immer neue Schwachstellen entdeckt werden. Dies macht kontinuierliche Überprüfungen auf Schwachstellen erforderlich. Gleichzeitig nehmen Umfang, Komplexität und Abhängigkeit von den installierten ITK-Systemen kontinuierlich zu. Deshalb sollte

die Wirkung des Sicherheitsmanagements mit seinen Konzepten und Maßnahmen sowie deren Umsetzung regelmäßig geprüft werden. Hierzu dienen Penetrationstests. Es wird unterschieden in Black-Box-, Grey-Box- und White-Box-Penetrationstests.

Bei Black-Box-Penetrationstests erhält der Tester vom beauftragenden Unternehmen ausschließlich die Angabe des Angriffsziels, d. h. den Namen des beauftragenden Unternehmens und gegebenenfalls der anzugreifenden Systeme. Darüber hinaus erhält er keine weiteren Informationen. Das Angriffsziel stellt sich für den Tester hier als eine Black-Box dar, deren Inhalt er nicht kennt. Er befindet sich somit in der gleichen Situation wie ein potenzieller Angreifer.

*Black-Box-
Penetrationstest*

Bei Grey-Box-Penetrationstests erhält der Tester Teilinformationen über das Angriffsziel, z. B. die eingesetzte Hardware und die Betriebssysteme. Er kann dadurch gezielter vorgehen, da er z. B. bekannte Schwachstellen dieser Systeme berücksichtigen kann.

*Grey-Box-
Penetrationstest*

Bei White-Box-Penetrationstests ist der Tester über die eingesetzten Informationssysteme, die Infrastruktur und die unternehmensinternen Regelungen und Maßnahmen informiert. Er verfügt somit über Insiderwissen und kann gezielte Angriffe fahren. Hierdurch sind sehr umfassende Penetrationstests möglich.

*White-Box-
Penetrationstest*

Die Durchführung von Penetrationstests beinhaltet u. a. die Informationssammlung über das Angriffsziel, z. B. über das Internet und über Ausspionieren vor Ort. Bei IT-Systemen kommt hinzu: das Scannen der Systeme, die Nutzung bekannter Schwachstellen der Zielsysteme etc.

14.1.3 IT-Security-Scans

Bei Security-Scans im IT-Bereich werden als Tools Security-Scanner eingesetzt, die Systeme oder Netze auf Sicherheitslücken hin untersuchen. Hier gibt es sowohl frei erhältliche (Freeware) als auch kommerzielle Tools. Die verfügbaren Scanner erstrecken sich über verschiedene Betriebssysteme, das Internet und Wireless LANs (WLAN). Hierbei können u. a. Benutzerkonten und Passwortstärke ermittelt und eine weitere Vielzahl von Angriffen und Checks, z. B. Denial-of-Service-Checks, gefahren werden.

Bekannte Scanner sind u. a. SATAN (Security Administrators Tool for Analyzing Networks), SAINT (Security Administrator's Integrated Network Tool) und Nessus.

Das deutsche BSI bietet auf seiner Webseite seit 2005 die „BSI Open Source Security Suite“ (BOSS) an [86]. Hierbei handelt es sich um eine Prüfsoftware, die der zentralen Sicherheitsprüfung von Computer-

netzen dient. BOSS baut im Wesentlichen auf Nessus auf und verfügt zusätzlich über eine leicht bedienbare deutschsprachige Bedienoberfläche sowie über den „Security Local Auditing Daemon“ (SLAD). Dieser übernimmt die Steuerung der angebundenen lokalen Sicherheitssoftware. „Für Nessus existieren derzeit über 7.000 Plugins für die Prüfung auf verschiedenste Sicherheitslücken [...] SLAD steuert [...] die [...] Sicherheitsmodule“ Chkrootkit, ClamAV Antivirus, John-The-Ripper, LSOFF, TIGER und Tripwire. Die BOSS-Live-CD enthält angabegemäß weitere freie Sicherheitssoftware, wie netcat, ngrep und ntop zur Nutzung unter dem Betriebssystem KNOPPIX.

Seit Dezember 2006 ist die Version 2.0 von BOSS freigegeben. Der BSI-Pressemittteilung zufolge ermöglicht sie schnellere Sicherheitsprüfungen sowie „die zentrale Verteilung und Konfiguration der Sicherheitssoftware auf den Linux-Clients im Netzwerk“. Sie verfügt darüber hinaus über eine einfachere Benutzeroberfläche.

14.2 Sicherheitscontrolling

Ein wesentlicher Bestandteil des Sicherheitsmanagements ist – wie bei allen Führungssystemen – die Regelung, d. h. das Sicherheitscontrolling. Vergleichen Sie dies mit Ihrer Haushaltskasse. Sie wissen, wie viel Geld Sie monatlich zur Verfügung haben, kennen Ihre regelmäßigen Ausgaben, z. B. für Ernährung, Miete, Pkw und wissen, was Sie sich mittel- bis langfristig anschaffen möchten. Hiervon ausgehend setzen Sie sich Ziele, z. B. Geld sparen, und legen die monatliche Sparrate fest. In der Folge prüfen Sie, wie weit Sie bei der Erreichung Ihrer Sparziele gekommen sind und entscheiden sich gegebenenfalls, Ziele zu verändern, Anschaffungen früher zu tätigen etc. Sie haben somit einen Regelkreis geschaffen, mit dem Sie Ihr eigenes Verhalten steuern.

*Sicherheits-
regelkreis*

Ein solcher Regelkreis ist auch für das Sicherheitsmanagement notwendig, um das Sicherheitsniveau den Anforderungen Ihres Unternehmens entsprechend anpassen und steuern zu können. Darüber hinaus schaffen Sie hiermit Transparenz, denn neben diesen regelnden und steuernden Möglichkeiten haben Sie einen Überblick über die Sicherheitssituation im Unternehmen und können dem Management die Situation, Trends etc. regelmäßig und aktuell berichten.

Der Sicherheitsregelkreis beginnt damit, dass die Zuständigen eine Planungsbasis allgemeiner Sicherheitsziele schaffen. Anschließend stimmen sie konkrete Ziele ab, vereinbaren diese und nehmen eine Detailplanung vor. In der Folge erhebt der Sicherheitsverantwortliche regelmäßig den aktuellen Status, vergleicht ihn mit dem Plan und

erstellt eine Prognose. Er analysiert Abweichungen, korrigiert gegebenenfalls die Prognose und ergreift bzw. initiiert bei Bedarf Korrekturmaßnahmen.

In grafischer Darstellung ergibt sich der folgende Regelkreis:

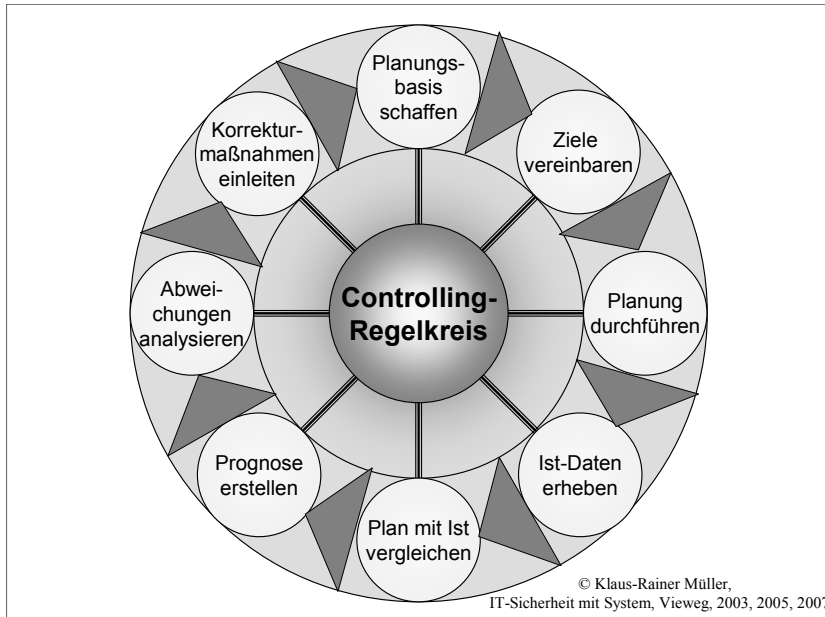


Abb. 14.2: Sicherheitsregelkreis

Welche Inhalte und Aufgaben verbergen sich nun hinter den einzelnen Elementen des Regelkreises? Beginnen wir mit der Planungsgrundlage. Sie lässt sich ermitteln, indem Sie sich die folgenden Fragen beantworten:

*Planungs-
grundlage*

- Welche generellen Sicherheitsziele hat das Unternehmen?
- Welche Teilziele leiten sich aus den generellen Zielen ab?
- Zu welchen Terminen (Meilensteinen) sollen diese Teilziele erreicht sein?
- In welchen Intervallen sollen Plan-Ist-Vergleiche durchgeführt werden?
- Welche Messkriterien gibt es für die Erreichung der Ziele und Teilziele?

Hieraus kann das Management überblicksartige Vorstellungen darüber entwickeln, welche Ziele kurz-, mittel- und langfristig erreicht

werden sollen. Ziele können beispielsweise sein, ein systematisches Sicherheits-, Kontinuitäts- und Risikomanagementsystem aufzubauen, Schutzbedarfsanalysen zu konzipieren und einzuführen, ein Berichtswesen einzuführen, den aktuellen Sicherheitsstatus zu ermitteln und Maßnahmen zur Behebung von Schwachstellen einzuleiten etc.

Zielvereinbarungsprozess

Aus diesen überblicksartigen Zielen müssen konkret messbare Teilziele abgeleitet, abgestimmt und vereinbart werden. Dies erfolgt im Zielvereinbarungsprozess. Ein konkret messbares Ziel kann beispielsweise sein, dass die Sicherheits-, Kontinuitäts- und Risikopolitik zum Bewertungszeitpunkt definiert, freigegeben und kommuniziert ist, dass das Notfall- und Katastrophenvorsorgehandbuch aktualisiert ist und eine Übung stattgefunden hat und dass bestimmte Sicherheitsprüfungen durchgeführt und die resultierenden Maßnahmen umgesetzt sind.

Planung

Im Anschluss hieran erfolgt die Planung, wann welche Teilziele (Meilensteine) erreicht sein sollen und wie die Erreichung gemessen werden kann. Die dazugehörigen Plandaten werden erfasst.

Plan-Ist-Vergleich

In zuvor definierten regelmäßigen Intervallen, z. B. monatlich, werden die aktuellen Ist-Daten erhoben. Diese werden im Plan-Ist-Vergleich einander gegenübergestellt. Auf Basis der Ist-Daten wird eine gegebenenfalls revidierte Prognose erstellt.

Abweichungsanalyse, Korrekturmaßnahmen

Auf der Basis dieser Ergebnisse lassen sich eine Abweichungsanalyse durchführen und – wenn erforderlich – Korrekturmaßnahmen ergreifen.

14.3 Berichtswesen (Safety-Security-Reporting)

Kontinuierlicher Überblick

Das Berichtswesen für die IT-Sicherheit (ISi-Berichtswesen), das Safety-Security-Reporting, hat zum Ziel, den Berichtsempfängern, z. B. dem Management, einen regelmäßigen Überblick über die Sicherheits- und Risikosituation des Unternehmens zu verschaffen. Dies erfordert die Erhebung der Anforderungen und daraus abgeleitet der Inhalte.

14.3.1 Anforderungen

Welche übergreifenden Anforderungen sind an ein solches Berichtswesen zu stellen? - Hierzu können folgende W-Fragen dienen: wer benötigt welche Informationen zu welchem Thema in welchem Detaillierungsgrad aus welcher Informationsquelle mit welcher Qualität und in welcher Form wann und wie oft von wem. Die Berichte sollten daher folgende qualitativen Eigenschaften erfüllen:

- empfängerorientiert
- informativ (strategisch, taktisch, operativ)
- angemessen detailliert
- nachweisbar
- standardisiert
- strukturiert
- präzise
- selbsterklärend, verständlich
- konsistent
- zeit- und ereignisgesteuert
- rechtzeitig
- zeitnah, aktuell.

*Eigenschaften
der Berichte*

Der Bericht sollte sich in Aufbau, Inhalt und Stil am Empfängerkreis orientieren. Management-Berichte sind knapp und allgemein verständlich. Sie beschränken sich auf wesentliche und übergreifende Informationen. Berichte an die operative Ebene sind in der Regel detaillierter und technischer oder fachspezifischer formuliert.

Ein Bericht sollte nur die geforderten und relevanten Informationen im entsprechenden Detaillierungsgrad wiedergeben. Die Motivation, einen Bericht zu lesen, reduziert sich mit seinem Umfang. Denken Sie an das Sprichwort „in der Kürze liegt die Würze“. Dies erfordert vom Autor des Berichts Abstraktionsvermögen und den Blick für das Wesentliche.

*Blick für das
Wesentliche*

Die Standardisierung der Berichte vereinfacht ihre Erstellung, da das „Rad nicht jedes Mal neu erfunden“ werden muss. Dem Empfänger erleichtert es das Lesen, da er die gewohnte Darstellung vorfindet und sich nur erstmalig in diese einfinden muss.

*Standardisie-
rung*

Die Struktur des Berichts ist ebenfalls wichtig, da eine sinnvolle und nachvollziehbar aufgebaute Gliederung das Verständnis und die Akzeptanz beim Empfänger erhöht.

Struktur

Wie jedes andere Dokument sollte auch ein Bericht präzise, verständlich und in sich konsistent sein. Die Verwendung von Kürzeln und Ähnlichem ist nur mit einer entsprechenden Erklärung sinnvoll, es sei denn, diese Kürzel sind für den Leserkreis in diesem Kontext eindeutig und bekannt.

Formulierung

Zeitgesteuert bedeutet, dass Berichte regelmäßig, z. B. monatlich oder quartalsweise erstellt werden. Darüber hinaus müssen bei sicherheitsrelevanten Ereignissen gegebenenfalls zusätzliche Berichte geschrieben und an bestimmte Empfängerkreise weitergeleitet werden.

*Berichts-
termine*

Rechtzeitigkeit Die rechtzeitige Lieferung heißt, dass diese Berichte z. B. jeweils am 5. Arbeitstag eines Monats beim Empfänger vorliegen. Hiermit verbunden ist die Zeitnähe und Aktualität der Informationen. Berichte, die den weit zurückliegenden Sicherheitsstatus wiedergeben, sind wenig hilfreich, um rechtzeitige Aktionen auszulösen.

Quantitative Anforderungen Die oben genannten qualitativen Anforderungen sollten konkretisiert werden. Hierzu gehört die Festlegung folgender Punkte des/der zu erstellenden Berichts/Berichte:

- Zielgruppe
- Ziel/Zweck des Berichts
- Inhalt
- Detaillierungsgrad
- genutzte Kennzahlen und Informationsbasen (Quellen), aus denen die Informationen für die Berichte extrahiert werden
- Layout (z. B. dreigeteilt: Graphik zur Visualisierung und zur Darstellung des zeitlichen Verlaufs (Plan, Ist, Abweichung, Prognose), Tabelle zur Hinterlegung der Graphik mit den zugrundeliegenden Daten, erläuternder Text/Interpretation der Ergebnisse/ergriffene Maßnahmen mit Verantwortlichen und Terminen)
- Frequenz (Stichtage)
- Aktualitätsgrad
- Verantwortlichkeit
- Länge der zu auszuwertenden Historie.

Anzahl und Umfang der zu berücksichtigenden zurückliegenden Daten bestimmen das Datenvolumen. Bei Großunternehmen erfordert dies oftmals den Einsatz von Datawarehouses (DWH) und Business Intelligence Tools (BI) zur Auswertung.



Tipp

Allgemein üblich sind Monatsberichte. Darüber hinaus sollten kurze Tagesberichte – idealerweise automatisch und elektronisch einsehbar – erstellt werden, die es dem CIO ermöglichen, morgens einen sofortigen Überblick über die aktuelle Situation der Informationsverarbeitung zu erhalten. Hierzu gehören insbesondere Ausfälle oder anderweitige Störungen des regulären Betriebs.

Matrix Es empfiehlt sich, für die Berichte eine Matrix zu erstellen, aus der ersichtlich ist, wer welche Informationen in welcher Qualität bis wann wie häufig an wen liefert und aus welcher Quelle diese Daten stammen.

14.3.2 Inhalte

Welche Inhalte können für einen IT-Sicherheitsbericht (Safety-Security-Report) relevant sein? Basis hierfür sind die primären Sicherheitskriterien Konformität, Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie die sekundären Sicherheitskriterien Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit. Hierzu sind Kennzahlen zu definieren, die über die Monate fortgeschrieben werden, sodass Veränderungen frühzeitig erkennbar sind.

Für jede Kennzahl des Berichts sind folgende Informationen relevant:

*Kennzahl-
charakteristika*

- Bezeichnung der Kennzahl
- Definition
- Bemerkungen
- Messziel
- Einheit
- Darstellungsform (z. B. Zahl, zeitlicher Verlauf, Balken-, Tortendiagramm)
- Art der Informationsgewinnung im Hinblick auf Messverfahren, Messpunkte, Messzeitpunkte und Messwerkzeug
- Qualität der Kennzahl im Hinblick auf Genauigkeit, Aktualität, Vollständigkeit, Konsistenz und Korrektheit
- Ziel-, Schwell- und Grenzwerte
- Betrachtete Systeme
- Berechnungsformel
- Aktualisierungshäufigkeit.

Von Interesse sind beispielsweise folgende Angaben, deren Bezeichnung sich an der Balanced Scorecard [11] orientiert:

- Finanzielle Perspektive
- Kundenperspektive
- Prozessperspektive
- Lern- und Entwicklungsperspektive.

In die finanzielle Perspektive fließt das Budget für das IT-Sicherheits-, IT-Kontinuitäts- und IT-Risikomanagement ein. Hier können die Plan- und Ist-Zahlen sowie die Prognose in Form einer Kurve dargestellt werden, aufgeteilt u. a. in Personalkosten, Beratungskosten, sicherheitsrelevante Hardware und Software. Eine eventuell verein-

*Finanzielle
Perspektive*

Kunden- perspektive

barte und erforderliche Pönale, z. B. bei Nichterfüllung der Verfügbarkeit, sollte dort ebenfalls ausgewiesen werden.

In die Kundenperspektive fließt die Erfüllung der sicherheits- und kontinuierkeitsrelevanten Leistungen ein. Hierzu gehört insbesondere der Vergleich zwischen Soll bzw. Plan und Ist, z. B. in Form der geforderten und der realisierten Verfügbarkeit. Von Interesse sind hierbei je nach Adressatenkreis u. a. folgende Leistungskennzahlen (Key Performance Indicator {KPI}), deren Wert monatlich fortgeschrieben und als Kurve dargestellt werden kann:

- Anzahl bzw. prozentualer Anteil der Informationssysteme je Verfügbarkeitsklasse und je Sicherheitsklasse
- Anzahl bzw. prozentualer Anteil der überwachten (monitored) Informationssysteme je Verfügbarkeitsklasse und je Sicherheitsklasse
- Anzahl der Ausfälle pro Informationssystem bzw. deren Verfügbarkeit
- Dauer der Ausfälle (Maximalwert, Minimalwert, Mittelwert, Spannweite/Range)
- Anzahl oder prozentualer Anteil der im Hinblick auf die Ausfallzeit und Verfügbarkeit eingehaltenen und nicht eingehaltenen SLAs
- durchschnittlich verbleibende Ausfallzeitreserve der Informationssysteme und minimale Ausfallzeitreserve unter Angabe des betroffenen Informationssystems
- Prozentualer Anteil der Informationssysteme, die einen Kontinuitätsplan besitzen sowie detaillierter Überblick
- Prozentualer Anteil der Informationssysteme, deren Kontinuitätsplan getestet wurde sowie detaillierter Überblick einschließlich Testergebnisbewertung
- Anzahl bzw. prozentualer Anteil der Informationssysteme, deren Kontinuitätsplan geübt wurde sowie detaillierter Überblick einschließlich Übungsergebnisbewertung
- Anzahl der Reviews des IT-Sicherheits-, -Kontinuitäts- und -Risikomanagements einschließlich betrachteter Prozesse, Systeme und Dienstleistungen sowie deren Kritikalität
- Anzahl der Antwortzeitüberschreitungen je Informationssystem
- Anzahl oder prozentualer Anteil der im Hinblick auf das Antwortzeitverhalten eingehaltenen und nicht eingehaltenen SLAs
- Zeitraum, der für die Einrichtung eines Benutzerkontos vergeht (minimal, durchschnittlich, maximal)
- ...

In der Prozessperspektive sind folgende Leistungskennzahlen (KPI) bzw. Informationen und deren Entwicklung von Monat zu Monat interessant, die ebenfalls in Kurvenform dargestellt werden kann:

*Prozess-
perspektive*

- Status der Hierarchieebenen der Sicherheitspyramide (Plan/Ist), z. B. Fertigstellungsgrad der Sicherheits-, Kontinuitäts- und Risikopolitik oder der Sicherheits- und Kontinuitätsrichtlinien sowie deren Anzahl (Plan/Ist)
- prozentuale Auslastung von Rechnern, Speichern, Netz und Druckern (Maximal-, Durchschnitts- und Minimalwert)
- Datenvolumen je Informationssystem
- Anzahl aller, neu angelegter, gelöschter, seit n Wochen inaktiver sowie gesperrter Benutzer
- Anzahl gesperrter Benutzer/Benutzerkonten (Accounts) pro Sperrgrund, z. B. Login fehlerhaft, Benutzer seit n Wochen inaktiv, ...
- Anzahl neu eingerichteter, geänderter und gelöschter Berechtigungen
- Anzahl erfolgreicher und fehlgeschlagener Logins
- Anzahl Passwortrücksetzungen
- Zeitraum, der vergeht, bis ein neues Benutzerkonto nach Erst-einrichtung zum ersten Mal genutzt wird (Maximalwert, Minimalwert, Mittelwert, Spannweite/Range)
- Zeitaufwand für die Einrichtung eines Benutzerkontos
- Anzahl erkannter und abgewehrter Viren (pro Virentyp)
- Anzahl erkannter, abgewehrter und erfolgreicher Angriffe
- Anzahl durchgeführter Risikoanalysen und der dabei gefundenen Schwachstellen
- ...

In die Lern- und Entwicklungsperspektive fließen Leistungskennzahlen über die Mitarbeiter ein. Hierzu gehört z. B.:

*Lern- und
Entwicklungs-
perspektive*

- Anzahl der Mitarbeiter im IT-Sicherheits-, -Kontinuitäts- und -Risikomanagement (insgesamt, intern und extern {jeweils Plan, Ist, Prognose})
- Fluktuationsrate
- Krankenstand
- Wissensspektrum
- ...

14.4 Safety-Security-Benchmarks

In Anbetracht der Kosten und hinsichtlich der eigenen Positionierung ist der „Blick über den Tellerrand“ hilfreich: Wo steht das Unternehmen im Vergleich mit anderen ähnlichen Unternehmen? Hierzu dienen Benchmarks, die sich auf bestimmte Themen, Teilbereiche oder die gesamte ITK beziehen können.

14.5 Hilfsmittel IT-Sicherheitsfragen

Grundlage für die Durchführung von Sicherheitsstudien bzw. Risikoanalysen bilden Fragenkataloge. Sie geben einen Rahmen und Umfang für die Sicherheitsstudie vor. Einen kleinen Auszug aus verschiedenen Themenbereichen bilden die folgenden Fragen:

- Sind die Sicherheitsanforderungen der Nutzer bekannt? – Sind diese Sicherheitsanforderungen ausreichend detailliert, z. B. im Hinblick auf Zugang, Zugriff, Verfügbarkeit, Datensicherung, Archivierung, Mengengerüst, Performance?
- Sind die Sicherheitsanforderungen nachvollziehbar dokumentiert? – Wenn ja, wie?
- Sind die ITK-Systeme nach ihrer Kritikalität je Sicherheitskriterium klassifiziert? – Wenn ja, welche Klassen gibt es?
- Wie erfolgte die Umsetzung der fachlichen Anforderungen in die ITK? – Wurden hierbei die erforderlichen PROSim-Elemente Prozesse, Ressourcen und Organisation betrachtet? – Wurden erforderliche Präventivmaßnahmen, z. B. Redundanz ergriffen? – Entsprechen diese in ihrer Art und Vollständigkeit den Anforderungen?
- Existieren die erforderlichen Datensicherungskonzepte? – Wie sehen die Datensicherungskonzepte aus? – Wie sieht das Auslageungsverfahren für Datensicherungen aus?
- Existieren für die ITK-Systeme den Sicherheitsanforderungen entsprechende Notfall- und Katastrophenvorsorgehandbücher?
- Existiert ein standardisiertes Antrags- und Genehmigungsverfahren für Zufahrt, Zutritt, Zugang und Zugriff?
- Werden die Anträge und die Genehmigungen nachvollziehbar dokumentiert und den erforderlichen Aufbewahrungsfristen entsprechend sicher aufbewahrt?
- ...

14.6 Zusammenfassung

Der Sicherheitsregelkreis unterstützt den Aufbau und die Anpassung des Sicherheits-, Kontinuitäts- und Risikomanagements an die kontinuierlichen Veränderungen innerhalb und außerhalb des Unternehmens.

*Sicherheits-
regelkreis*

Sicherheitsprüfungen sind Elemente des Regelkreises und können in Form von Sicherheitsstudien bzw. Risikoanalysen sowie Penetrationstests und Security-Scans durchgeführt werden. Durch sie können in einer Momentaufnahme Sicherheitsdefizite aufgedeckt und weiter gehende Schutzmaßnahmen empfohlen werden.

*Sicherheits-
prüfungen*

Durch das Sicherheitscontrolling werden Ziele definiert und ihr Erreichungsgrad unterjährig verfolgt. Monatliche und Adhoc-Berichte dienen als nachvollziehbare Dokumentation der aktuellen Sicherheitssituation. Die Gliederungsstruktur der Monatsberichte kann sich an der Balanced Scorecard orientieren und die finanzielle, Kunden-, Prozess- sowie Lern- und Entwicklungsperspektive beinhalten.

*Sicherheits-
controlling,
Berichtswesen*

In Safety-Security-Benchmarks können Vergleiche mit anderen Unternehmen durchgeführt werden.

*Safety-Security-
Benchmark*

15 Reifegradmodell des Sicherheitsmanagements – Safety/Security/Continuity Management Maturity Model

Häufig stellt sich in Unternehmen die Frage, welches Niveau das Sicherheitsmanagement erreicht hat und wie es sich bewerten lässt. In diesen Fällen hilft ein Reifegradmodell des Sicherheitsmanagements (Safety, Security and Continuity Management Maturity Model).

Zur Bewertung des Sicherheitsmanagements gibt es verschiedene Ansätze mit unterschiedlichem Fokus. Das Systems Security Engineering – Capability Maturity Model® [87] konzentriert sich auf die Prozesse, die zur Erreichung der IT-Sicherheit erforderlich sind, sowie auf die 5 Reifegradstufen. Es betrachtet den kompletten Lebenszyklus sicherer Produkte und Systeme.

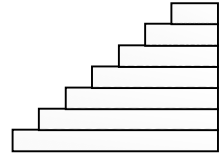
Das Federal Information Technology Security Assessment Framework [88] des NIST kennt ebenfalls fünf Level. Es betrachtet die Sicherheitspolitik, Prozeduren zu ihrer Implementierung, die Implementierung und Prüfung bis hin zu einem umfassenden und integralen Sicherheitsprogramm.

Das Security-Maturity-Modell in [89] beinhaltet drei Ebenen, deren letzte die evolutionäre Ebene ist.

Das Reifegradmodell des Autors für das Sicherheitsmanagement, das Safety, Security and Continuity Management Maturity Model {SSCMMM} nach Dr.-Ing. Müller, orientiert sich an der Sicherheitspyramide und leitet hieraus die verschiedenen Reifegradstufen ab.

Das Kapitel behandelt folgende Themen:

1. Systems Security Engineering – Capability Maturity Model®
2. Federal Information Technology Security Assessment Framework
3. Security-Maturity-Modell
4. Reifegradmodell nach Dr.-Ing. Müller:
Safety, Security and Continuity Management Maturity Modell
5. Checkliste Reifegrad
6. Praxisbeispiel
7. Zusammenfassung



15.1 Systems Security Engineering – Capability Maturity Model®

Prozess-Referenzmodell

Das Systems Security Engineering – Capability Maturity Model® [87] (SSE-CMM®) (ISO/IEC 21827:2002) ist ein Prozess-Referenzmodell. Es fokussiert sich auf jene Anforderungen, die erforderlich sind, um Sicherheit in einzelne oder zusammenhängende IT-Systeme zu implementieren. Der Schwerpunkt liegt auf der Prozesssicht, d. h. den Prozessen, die zur Erreichung der IT-Sicherheit erforderlich sind, sowie auf deren Reifegrad. Hierbei liegt der komplette Lebenszyklus sicherer Produkte und Systeme von der Konzeptdefinition über die Anforderungsanalyse, Design, Entwicklung, Integration, Installation, Betrieb und Wartung bis hin zur Außerbetriebnahme im Fokus.

Engineering-Prozess

SSE-CMM® unterteilt den Security-Engineering-Prozess in drei Basisbereiche: Risiko-, Engineering- und Sicherungsprozess.

Risiko-, Security-Engineering- und Sicherungsprozess

Im Risikoprozess werden Bedrohungen, Schwachstellen und deren Auswirkungen betrachtet. Der Security-Engineering-Prozess durchläuft die Phasen Konzept, Design, Implementierung, Test, Verteilung, Betrieb, Wartung und Außerbetriebnahme. Der Sicherungsprozess konzentriert sich auf das Vertrauen in die Wiederholbarkeit der Ergebnisse des Security-Engineering-Prozesses. Je reifer eine Organisation ist, desto wahrscheinlicher ist es, dass sie wieder zu den gleichen Ergebnissen gelangt. Außerdem stellt der Prozess das Vertrauen dafür her, dass die implementierten Kontrollen die erwarteten Risiken reduzieren.

Architektur des SSE-CMM®

Die Architektur des SSE-CMM® soll die Bestimmung des prozessualen Reifegrads einer Security-Engineering-Organisation ermöglichen. Ziel ist es hierbei, grundlegende Charakteristiken des Security-Engineering-Prozesses von Management- und Institutionalisierungs-Charakteristiken zu trennen. Daher verfügt das Modell über die zwei Dimensionen Domäne/Gebiet (domain) und Fähigkeit (capability).

Die Dimension Domäne besteht aus all jenen Praktiken, die insgesamt das Security-Engineering definieren und für dieses spezifisch sind. Diese werden als Basispraktiken bezeichnet. Die Dimension Fähigkeit repräsentiert jene Praktiken, die Indizien für die Fähigkeit zum Prozessmanagement und zur Institutionalisierung darstellen. Diese Praktiken werden als generische Praktiken bezeichnet, da sie sich in einer Vielzahl von Bereiche anwenden lassen.

Basispraktiken

Das SSE-CMM® umfasst 129 Basispraktiken, die in 22 Prozessbereichen organisiert sind. 61 Basispraktiken in 11 Prozessbereichen umfassen die Hauptgebiete des Security-Engineering. Die verbleibenden

68 Basispraktiken, ebenfalls in 11 Prozessbereichen, adressieren die Gebiete Projekte und Organisation.

Generische Praktiken sind zu logischen Gebieten gruppiert, die in fünf Fähigkeitsebenen unterteilt sind. Im Gegensatz zu den Basispraktiken sind die generischen Praktiken nach ihrem Reifegrad sortiert.

*Generische
Praktiken*

Die fünf Reifegrad-Ebenen lauten:

Reifegrade

Level 1: „Performed informally“

Level 2: „Planned and Tracked“

Level 3: „Well Defined“

Level 4: „Quantitatively Controlled“

Level 5: „Continuously Improving“

15.2 Information Technology Security Assessment Framework

Das Federal Information Technology Security Assessment Framework [88] des NIST kennt die folgenden 5 Level:

Reifegrade

Level 1: Documented Policy

Level 2: Documented Procedures

Level 3: Implemented Procedures and Controls

Level 4: Tested and Reviewed Procedures and Controls

Level 5: Fully integrated Procedures and Controls.

Die Level-1-Kriterien beschreiben die Komponenten einer Sicherheitspolitik. Level 2 beinhaltet formale, vollständige und gut dokumentierte Prozeduren zur Implementierung der Sicherheitspolitik aus Level 1. Auf Level 3 sind die IT-Sicherheitsprozeduren und -kontrollen konsistent zueinander implementiert und trainiert. Level 4 des Rahmenwerks beinhaltet die regelmäßige Prüfung der Angemessenheit und Effektivität der Sicherheitspolitik, -prozeduren und -kontrollen sowie effektiver Korrekturmaßnahmen zur Adressierung identifizierter Schwachstellen. Zu Level 5 des Rahmenwerks gehört ein umfassendes Sicherheitsprogramm, das integraler Bestandteil der Organisationskultur ist. Entscheidungen basieren auf Kosten, Risiken und Auswirkungen. Es erfolgt eine Orientierung am Lebenszyklus. Best Practices werden kontinuierlich identifiziert und institutionalisiert. Metriken über den Status des Sicherheitsprogramms sind etabliert und erfüllt.

*Inhalte/
Kriterien der
Level 1 bis 5*

15.3 Security-Maturity-Modell

Das Security Maturity Model nach [89] umfasst die folgenden vier Level:

Level 0: Blind Trusting

Level 1: Ad hoc tries

Level 2: Policy

Level 3: Evolutionary

Die drei Übergänge von einer Stufe zur nächsten erfordern jeweils umgesetzte Konzepte zuerst für Awareness (Bewusstsein), dann für die Organisation und abschließend auf Prozessebene.

15.4 Reifegradmodell nach Dr.-Ing. Müller

Das hier für das Sicherheitsmanagement (Safety, Security, Continuity) ausgeprägte, aber allgemein anwendbare Reifegradmodell des Autors umfasst die im folgenden angegebenen Stufen (level). Die jeweils höhere Stufe setzt die Anforderungserfüllung der vorangegangenen Stufe voraus. Die Bezeichnung der jeweiligen Stufe gibt Auskunft darüber, in welchem Status sich das Sicherheitsmanagement dieser Stufe befindet:

Stufe 0: unbekannt (unknown)

Stufe 1: begonnen (initiated, started)

Stufe 2: konzipiert (designed)

Stufe 3: standardisiert (standardized)

Stufe 4: integriert (integrated)

Stufe 5: gesteuert (managed)

Stufe 6: selbstlernend (self-teaching)

15.4.1 Stufe 0: unbekannt

Diese Stufe ist dadurch gekennzeichnet, dass es im Unternehmen kein durchgängiges Bewusstsein für das Thema Sicherheit gibt. Das Management stellt keine personellen und/oder finanziellen Ressourcen bereit, um Sicherheitsmaßnahmen ergreifen zu können. Wenn Sicherheitsmaßnahmen ergriffen worden sind, so ist dies individuellem Engagement zu verdanken, aber keine vom Unternehmen bewusst initiierte Maßnahme.

15.4.2 Stufe 1: begonnen

Auf dieser Stufe sind eine Vielzahl von Sicherheitsmaßnahmen vom Unternehmen bewusst initiiert und umgesetzt worden. Es gibt ein generelles Sicherheitsbewusstsein im Unternehmen. Für die ITK-Sicherheit werden personelle und finanzielle Ressourcen eingesetzt.

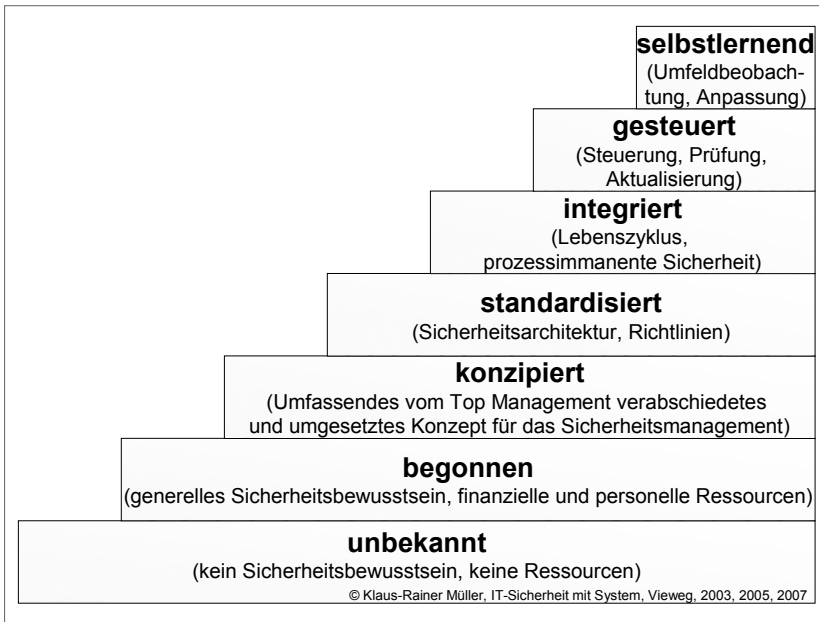


Abb. 15.1: Reifegradmodell nach Dr.-Ing. Müller

15.4.3 Stufe 2: konzipiert

Es existiert ein vom Top Management verabschiedetes, kommuniziertes und umgesetztes Konzept, wie das Sicherheits-, Kontinuitäts- und Risikomanagement im Unternehmen wahrgenommen werden soll. Dies beinhaltet eine am Markt und der Unternehmensstrategie ausgerichtete Sicherheits-, Kontinuitäts- und Risikopolitik, Sicherheits- und Kontinuitätsziele, -konzepte und -maßnahmen. Bei den genannten Themen werden die Themenfelder Prozesse, Ressourcen und Organisation berücksichtigt.

15.4.4 Stufe 3: standardisiert

Die verschiedenen Sicherheitsmaßnahmen und -konzepte sind in Form von Richtlinien standardisiert und umgesetzt. Für die wesentlichen Themenfelder existieren derartige Richtlinien. Der Schutzbedarf

von Geschäftsprozessen und Informationssystemen wird auf standardisierte Weise erhoben. Die Geschäftsprozesse und Informationssysteme sind entsprechend ihrem Schutzbedarf klassifiziert. Es existiert eine Sicherheitsarchitektur, in der die anwendbaren Sicherheitselemente bezogen auf Prozesse, Ressourcen und Organisation sowie der aktuelle Status enthalten sind.

15.4.5 Stufe 4: integriert

Das Sicherheits-, Kontinuitäts- und Risikomanagement ist in den gesamten Lebenszyklus der Prozesse, Ressourcen, Produkte und Dienstleistungen so integriert, dass bereits ab der ersten Phase der Idee Sicherheitselemente berücksichtigt werden. Die Sicherheits- und Kontinuitätselemente werden über alle Phasen des Lebenszyklus weiter verfeinert. Im Hinblick auf die ITK bedeutet dies, dass Sicherheits- und Kontinuitätselemente von der Phase der Idee über die Machbarkeit, die Konzeption, die Entwicklung, den Test und den Betrieb bis hin zur Außerbetriebnahme berücksichtigt werden.

15.4.6 Stufe 5: gesteuert

Das Sicherheits-, Kontinuitäts- und Risikomanagement verfügt über einen Regelkreis, mit dem es kontinuierlich nachvollziehbar verfolgt und gesteuert wird. Dies beinhaltet die regelmäßige und geplante Aktualisierung der Sicherheits- und Kontinuitätsanforderungen sowie die Verifizierung im Hinblick auf Umsetzung und Wirksamkeit der Sicherheits- und Kontinuitätselemente.

15.4.7 Stufe 6: selbst lernend

Auf der obersten Stufe entwickelt sich das Sicherheits-, Kontinuitäts- und Risikomanagement (pro)aktiv kontinuierlich weiter. Dies beinhaltet die kontinuierliche Marktbeobachtung z. B. im Hinblick auf neue Bedrohungen, Technologien etc. Die entsprechenden Verantwortlichkeiten sind nachvollziehbar Funktionen im Unternehmen zugeordnet.

15.5 Checkliste Reifegrad

Wie können Sie selbst beurteilen, auf welcher Stufe sich das Sicherheitsmanagement, welches hier das Kontinuitätsmanagement und das Risikomanagement beinhaltet, in Ihrem Unternehmen befinden? Hierzu können Sie den folgenden Fragenkatalog verwenden, der Ihnen einen ersten Überblick verschafft. Diese erste Einstufung lässt

sich im Anschluss durch detailliertere Fragebögen schrittweise weiter präzisieren.

Stufe	Kontrollen (Controls) auf Detaillierungsebene 1 (Überblick)
0	Im Unternehmen fehlt ein durchgängiges Sicherheits-, Kontinuitäts- und Risikobewusstsein.
	Personelle und/oder finanzielle Ressourcen für Sicherheits- und Kontinuitätsmaßnahmen werden vom Management nicht bereit gestellt.
	Das Unternehmen initiiert keine Sicherheits- und Kontinuitätsmaßnahmen.
1	Im Unternehmen existiert über alle Ebenen ein vom Top Management initiiertes allgemeines Sicherheits-, Kontinuitäts- und Risikobewusstsein.
	Das Unternehmen stellt personelle und finanzielle Ressourcen für Sicherheits- und Kontinuitätsmaßnahmen zur Verfügung.
	Das Unternehmen hat weitestgehend Sicherheits- und Kontinuitätsmaßnahmen initiiert und umgesetzt.
2	Für das Sicherheits-, Kontinuitäts- und Risikomanagement (SKRM) im Unternehmen existiert ein vom Top Management verabschiedetes, kommuniziertes und im Unternehmen umgesetztes Konzept.
	Das SKRM beinhaltet die am Markt und an der Unternehmensstrategie ausgerichtete Sicherheits-, Kontinuitäts- und Risikopolitik, Sicherheits- und Kontinuitätsziele, -konzepte und -maßnahmen.
	Das SKRM erstreckt sich auf die Themenfelder Prozesse, Ressourcen und Organisation sowie auf alle Sicherheitskriterien.
3	Sicherheits- und Kontinuitätsmaßnahmen und -konzepte sind in Form von Richtlinien in allen wesentlichen Themenfeldern (Prozesse, Ressourcen und Organisation) standardisiert, kommuniziert, geschult und umgesetzt.
	Die Sicherheits- und Kontinuitätsanforderungen der Prozesse werden auf standardisierte Weise erhoben und diese entsprechend ihrem Schutzbedarf klassifiziert. Die Anforderungen werden auf die Schutzobjekte transformiert.
	Es existiert eine Sicherheits-, Kontinuitäts- und Risikoarchitektur, in der die anwendbaren Sicherheits- und Kontinuitätselemente bezogen auf Prozesse, Ressourcen und Organisation sowie der aktuelle Status der Sicherheits-, Kontinuitäts- und Risikoarchitektur enthalten sind.

4	Sicherheits- und Kontinuitätselemente sind in alle Phasen des Lebenszyklus von Prozessen, Ressourcen, Produkten und Dienstleistungen integriert.
	Die Sicherheits- und Kontinuitätselemente beinhalten die Themenfelder Prozesse, Ressourcen und Organisation.
	Die Sicherheits- und Kontinuitätselemente orientieren sich an den Anforderungen und Richtlinien.
5	Für das SKRM existiert ein Prozess, eine Organisation und ein Regelkreis, mit Hilfe dessen es kontinuierlich nachvollziehbar verfolgt und gesteuert wird. Die Verfolgung und Steuerung erfolgt anhand von Plan-Ist-Vergleichen, Prognosen, Analysen und Korrekturmaßnahmen.
	Das SKRM umfasst die regelmäßige und geplante Aktualisierung der Sicherheits- und Kontinuitätsanforderungen.
	Im Rahmen des SKRMs erfolgt die regelmäßige Planung sowie die Überprüfung der Umsetzung und der Wirksamkeit der Sicherheits- und Kontinuitätselemente.
6	Das SKRM beinhaltet Funktionen und/oder Rollen, die für dessen kontinuierliche (pro)aktive Weiterentwicklung verantwortlich sind.
	Das SKRM entwickelt sich nachvollziehbar und messbar weiter. Dies umfasst die Themenfelder Prozesse, Ressourcen und Organisation sowie die Lebenszyklen.
	Das SKRM beinhaltet nachvollziehbare und wirksame Methoden und Verfahren, die sicherstellen, dass aktuelle Entwicklungen frühzeitig erkannt, bewertet, aufgegriffen und bei Bedarf anforderungsgerecht umgesetzt werden können.

15.6 Praxisbeispiel

Das Musterunternehmen beauftragt eine externe Unternehmensberatung mit einer Sicherheitsprüfung eines neuen Informationssystems, dessen Entwicklung an ein Softwarehaus vergeben wurde. Als Ergebnis der Sicherheitsstudie ergibt sich, dass

- das Unternehmen eine Vielzahl unterschiedlicher Sicherheits- und Kontinuitätsmaßnahmen zur Absicherung des IT-Betriebs ergriffen hat
- Sicherheitsrichtlinien für Passwörter existieren,
- in die Konzeption des neuen Informationssystems verschiedene Sicherheits- und Kontinuitätsmaßnahmen eingeflossen sind

- Sicherheits- und Kontinuitätsanforderungen für das neue Informationssystem nicht erhoben wurden
- das Management und alle Mitarbeiter ein ausgeprägtes Sicherheits- und Kontinuitätsbewusstsein haben
- das Management die erforderlichen personellen und finanziellen Ressourcen zur Erreichung des geforderten Sicherheits- und Kontinuitätsniveaus bereitstellt
- das externe Softwarehaus im Vorfeld der Auftragsvergabe im Hinblick auf Qualitäts- und Sicherheitsstandards begutachtet wurde.

Das Musterunternehmen befindet sich auf der Stufe 1, begonnen, weil die dort geforderten Anforderungen erfüllt sind.

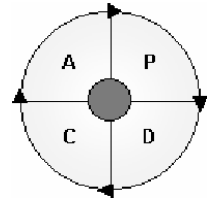
15.7 Zusammenfassung

Zur Reifegradbestimmung der IT-Sicherheit existieren u. a. das Systems Security Engineering – Capability Maturity Model® (ISO/IEC 21827:2002), ein Prozess-Referenzmodell, und das fünfstufige Reifegradmodell des NIST in Form des Federal Information Technology Security Assessment Framework.

Mit dem Reifegradmodell des Autors können Sie das Sicherheits-, Kontinuitäts- und Risikomanagement anhand von 7 Stufen, beginnend bei Stufe 0, bewerten. Die Stufen charakterisieren über ein Eigenschaftswort das erreichte Niveau. Ausgangspunkt ist die Stufe 0, „unbekannt“, gefolgt von den Stufen „begonnen“, „konzipiert“, „standardisiert“, „integriert“ und „gesteuert“. Die oberste Stufe bezeichne ich als „selbst lernend“. Voraussetzung für den Übergang in die jeweils nächste Stufe ist, dass alle dort definierten Anforderungen sowie die der darunter liegenden Stufen erfüllt sind.

16 Sicherheitsmanagementprozess

Die bisherigen Kapiteln haben den hierarchischen Aufbau der Sicherheitspyramide, die PROSim-Elemente, die Integration von Sicherheitselementen in die Lebenszyklen sowie den Sicherheitsregelkreis beschrieben. Hieraus lässt sich der Sicherheitsprozess bzw. Sicherheitsmanagementprozess bzw. Sicherheits-, Kontinuitäts- und Risiko-managementprozess eines Unternehmens formen, indem diese Elemente in einem Ablauf zusammengeführt werden. Was ist hierbei zu beachten?



16.1 Deming- bzw. PDCA-Zyklus

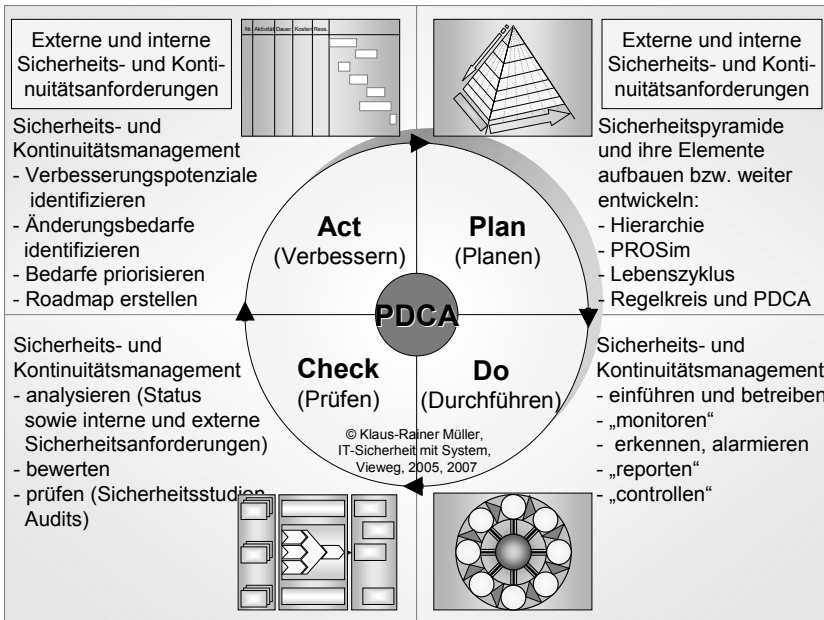


Abb. 16.1: Sicherheitsmanagementprozess nach Dr.-Ing. Müller

Wie bereits erwähnt ist Sicherheit ein bewegliches Ziel, da sich Sicherheits- und Kontinuitätsanforderungen, Bedrohungen und Schwachstellen kontinuierlich verändern. Um dem Rechnung zu tragen, sollte der Sicherheitsmanagementprozess einen kontinuierlichen Verbesserungsprozess enthalten. Hierzu lässt sich der Deming-

bzw. PDCA-Zyklus nutzen, der aus dem Qualitätsmanagement bekannt ist [29]. PDCA steht für die vier Phasen Plan-Do-Check-Act.

Der Aufbau eines Informations-, eines ITK- bzw. eines umfassenden Sicherheitsmanagementsystems (ISMS, ICTSMS, SMS), beginnt dementsprechend mit der Planung (Plan). Hieran schließt sich die Umsetzung (Do) einschließlich Test, Pilotierung und Betrieb mit Monitoring, Reporting und Controlling an. In der Überwachungsphase (Check) erfolgt die Analyse, Bewertung und Überprüfung des Systems. Die letzte Phase der Verbesserung (Act) wertet die Ergebnisse aus. Sie leitet hieraus Verbesserungsmaßnahmen für den Einstieg in die nächste Planung und den nächsten Durchlauf des PDCA-Zyklus ab.

Hinter dem Begriff Sicherheitsmanagementsystem, ob vollständig, für Informationen oder die ITK kann sich dabei – wie bei der Sicherheitspyramide – ein Sicherheits-, Kontinuitäts- und Risikomanagementsystem (ISKRMS, ITKSKRMS, ICTSKRMS bzw. SKRMS) verbergen.

16.2 Planung

Plan: Verantwortliche festlegen

Zu Beginn der Planungsphase eines Sicherheits-, Kontinuitäts- und Risikomanagementsystems (SKRMS) ernennt die Geschäftsleitung den erforderlichen Rollen und der Unternehmensgröße entsprechend den Chief Compliance Officer (CCO), den Chief Security Officer (CSO), den Chief Risk Officer (CRO) und den Chief Information Security Officer (CISO) und legt ihre Aufgaben und Verantwortlichkeiten fest. Das Organigramm des Unternehmens erfährt eine dementsprechende Erweiterung.

Sicherheits-, Kontinuitäts- und Risikopolitik definieren, SKRM-Prozess festlegen

CCO, CSO, CRO und CISO stellen die externen Anforderungen zusammen, z. B. aus Gesetzen, aufsichtsbehördlichen Bestimmungen, Normen und Standards sowie abgeschlossenen Verträgen. Sie entwickeln das Vorgehensmodell zum Aufbau des Sicherheits-, Kontinuitäts- und Risikomanagements anhand der Sicherheitspyramide des Autors. Sie legen den SKRM-Prozess fest und bereiten die prinzipiellen Inhalte der Sicherheits-, Kontinuitäts- und Risikopolitik bis hin zu den Mindestszenarien vor. CCO, CSO, CRO und CISO stimmen die Sicherheits-, Kontinuitäts- und Risikopolitik des Unternehmens mit der Geschäftsleitung ab, die sie freigibt.

Sicherheits- und Kontinuitätsanforderungen erheben

CSO, CRO und CISO legen konsistente Klassen für Sicherheit, Kontinuität und Risiko fest. Gemeinsam mit den Prozessverantwortlichen erheben sie die Sicherheits- und Kontinuitätsanforderungen der Prozesse bzw. lassen diese aufnehmen, wobei sie die Prozessarchitektur des Unternehmens zugrunde legen. Die Erhebung erfolgt im Rahmen

von Business und Operational Impact Analysen. Als Ergebnis liegen die entsprechenden Berichte bzw. Informationen vor. Die Ergebnisse lassen sich außerdem zum Nachjustieren der Sicherheits-, Kontinuitäts- und Risikoklassen nutzen.

Die anschließende Transformation bildet Sicherheits- und Kontinuitätsklassen auf Sicherheits- und Kontinuitätscharakteristika von Ressourcen, Support- und Begleitprozessen ab. Ein gegebenenfalls erforderlicher weiterer Schritt transformiert darüber hinausgehende spezielle Sicherheits- und Kontinuitätsanforderungen.

Sicherheits- und Kontinuitätsanforderungen transformieren

Die Sicherheits- und die Kontinuitätsverantwortlichen stellen die Mindestszenarien, die Sicherheits- und Kontinuitätsanforderungen, das Bedrohungspotenzial, die Sicherheitscharakteristika, die Risikomatrix, Prozess- und Ressourcenarchitekturen sowie Netztopologien zusammen. Diese bilden die Basis zur Entwicklung der Sicherheits- und Kontinuitätsarchitektur. Sie umfasst die Liste der prinzipiell betrachteten Bedrohungen, der Sicherheits- und Kontinuitätsanforderungen sowie der Sicherheits- und Kontinuitätselemente für Betriebs- und Angriffssicherheit sowie für Kontinuität für Prozesse, Ressourcen, Organisation, Dienstleistungen und Produkte. Ferner wird die derzeitige Architektur in Form beispielsweise von Systemarchitekturen und Netztopologien dargestellt.

Sicherheits- und Kontinuitätsarchitektur aufbauen

Für die Sicherheits- und Kontinuitätselemente entwickeln die Sicherheits- und die Kontinuitätsverantwortlichen bei Bedarf übergreifende Richtlinien. Solche Elemente können beispielsweise Datenschutz, Zufahrts-, Zutritts-, Zugangs- und Zugriffsschutz, Datensicherung, Notfall- und Katastrophenvorsorgeplanung, Computerviren-Schutz, IT-, Internet- und E-Mail-Schutz sein. Nach der Erstellung entsprechender Richtlinien werden diese geprüft, verabschiedet und eingeführt.

Sicherheits- und Kontinuitätsrichtlinien erstellen

Die erstellten Sicherheits- und Kontinuitätsrichtlinien dienen als Basis für die Sicherheits- und Kontinuitätskonzepte, welche die Ressourcenspezifika, z. B. von Systemen, berücksichtigen.

Sicherheitskonzepte entwickeln

Die Umsetzung der Konzepte in Maßnahmen wird nachvollziehbar dokumentiert.

Maßnahmen durchführen

Die Sicherheits- und Kontinuitätsverantwortlichen tragen die Sicherheits- und Kontinuitätselemente sowie die prozess-, ressourcen-, produkt- und dienstleistungsspezifischen Lebenszyklen zusammen. Die verschiedenen Phasen der Lebenszyklen erhalten die erforderlichen Sicherheits- und Kontinuitätselemente mit entsprechenden Ergebnissen je Aktivität.

Sicherheit in die Lebenszyklen integrieren

*Regelkreis
aufbauen*

Die Sicherheits- und Kontinuitätsverantwortlichen bauen den Regelkreis auf. Dies beinhaltet die Festlegung von Kontrollelementen (controls) und Kennzahlen. Sie dienen als Basis für das spätere Monitoring, Controlling und Reporting sowie Prüfungen.

16.3 Durchführung

*Do:
Sicherheits-
management
betreiben und
monitoren*

In der nächsten Phase des PDCA-Zyklus erfolgt die Umsetzung (Do). Mitarbeiter erhalten Schulungen und werden sensibilisiert. Die jeweils operativ Zuständigen für Prozesse und Ressourcen, wie z. B. für den IT-Betriebsprozess, für Gebäude und Systeme, führen den Betrieb unter Berücksichtigung der eingeführten Sicherheits- und Kontinuitätskonzepte und -maßnahmen durch. Sie messen und überwachen (monitoring) den Betrieb den Anforderungen entsprechend kontinuierlich. Meldungen werden erkannt und ausgewertet, es wird alarmiert und auf Alarmer reagiert etc.

Den Anforderungen an das Controlling folgend sammelt der Bereich Informationsservices Controlling-Daten, führt Plan-Ist-Vergleiche durch, erstellt Prognosen, analysiert eventuelle Abweichungen und schlägt Korrekturmaßnahmen vor. Er dokumentiert die Controlling-Ergebnisse in regelmäßigen Berichten (reporting) und leitet sie an die jeweiligen Adressaten. Status, Maßnahmen und verbleibende Risiken kommunizierte er in geeigneter Form und in spezifischem Umfang an die entsprechenden internen und externen Bezugsgruppen. Diese Einbindung der Bezugsgruppen schafft Bewusstsein und angemessenes Vertrauen in das Sicherheits-, Kontinuitäts- und Risikomanagement.

16.4 Prüfung

*Check:
Sicherheits-
management
prüfen*

In regelmäßigen Abständen und bedarfsorientiert erfolgen Prüfungen (Checks) des Sicherheits-, Kontinuitäts- und Risikomanagements. Es werden Tests, Übungen und Sicherheitsprüfungen durchgeführt. Die Ergebnisse werden dokumentiert, analysiert, ausgewertet und berichtet.

16.5 Verbesserung

Neue Erkenntnisse in Entwicklung und Betrieb führen zu einer Rückkopplung in die entsprechenden Schritte des Sicherheitsmanagementprozesses bzw. Ebenen der Sicherheitspyramide oder des jeweiligen Lebenszyklus. Sie lösen Weiterentwicklungen aus. Dies gilt ebenso für Veränderungen der Umwelt, neue Gesetze, Produkte, u. ä. Beispielsweise macht ein neues Gesetz eine Ergänzung in den Anlagen zur Sicherheits-, Kontinuitäts- und Risikopolitik erforderlich. Hieraus ergeben sich dann Änderungen in den darunter liegenden Ebenen der Sicherheitspyramide bzw. den Folgeschritten im Sicherheitsmanagementprozess.

Act:
Sicherheits-
management
weiter-
entwickeln

Neue Prozesse und Ressourcen erfordern gegebenenfalls neue oder modifizierte Lebenszyklusmodelle. Kann jedoch ein bestehendes Lebenszyklusmodell genutzt werden, so erfolgt der Einstieg in den entsprechenden Schritt „Sicherheitsanforderungen erheben“ im Prozesslebenszyklus und zieht entsprechende Erhebungen und Aktivitäten in den folgenden Prozessschritten nach sich. Auch innerhalb des Lebenszyklus können sich Erkenntnisse ergeben, die Auswirkungen auf die Inhalte der Hierarchieebenen der Sicherheitspyramide haben. So z. B. die Anforderung von Sicherheitselementen, die über die bestehende Sicherheitsarchitektur hinausgehen.

Nachdem Verbesserungs- und Änderungsbedarfe identifiziert sind, erfolgt ihre Priorisierung. Die Roadmap stellt den zeitlichen Ablauf sowie die erforderlichen Ressourcen dar.

16.6 Zusammenfassung

Die folgende Tabelle zeigt die einzelnen Schritte des Prozesses Sicherheitsmanagement mit den dazugehörigen Eingangsinformationen, Methoden und Ergebnissen.

Eingangs- informationen	Aktivitäten unter Berücksichtigung von PROSim	Methoden	Ergebnisse
PLAN			
	Sicherheits- verantwortlichen benennen		Erweitertes Organi- gramm, Funktionsbe- schreibung, Aufga- benbeschreibung, Vollmachtenregelung

Eingangs- informationen	Aktivitäten unter Berücksichtigung von PROSim	Methoden	Ergebnisse
Sicherheits- und Kontinuitätsanforderungen, externe, z. B. durch Gesetze, Aufsicht, Normen, Standards, Best Practices, Wirtschaftsprüfer, sowie unternehmensspezifische	Sicherheits-, Kontinuitäts- und Risikopolitik festlegen		Sicherheits-, Kontinuitäts- und Risikopolitik mit Vorgehensmodell sowie Anlagen für Gesetze und Vorgaben, Normen und Standards, sowie Mindestszenarien
Prozess- und Ressourcenarchitektur, Leistungs- und Produktportfolio	Sicherheits- und Kontinuitätsanforderungen erheben	SBAs, BIAs, OIAs	Sicherheits-, Kontinuitäts- und Risikoklassen, Sicherheits- und Kontinuitäts – anforderungen
Sicherheits- und Kontinuitätsanforderungen und -klassen aus BIAs	Sicherheits- und Kontinuitätsanforderungen transformieren auf Schutzobjekte	HoSSC, SSCFD	Sicherheits- und Kontinuitätscharakteristika der Schutzobjekte
Sicherheits- und Kontinuitätsanforderungen und -charakteristika, Prozess- und Ressourcenarchitektur, z. B. Systemarchitektur, Netztopologie, Gebäude-, Verkaufspläne, ...	Sicherheits- und Kontinuitäts- sowie Risikoarchitektur aufbauen		Prinzipielle Bedrohungen, Sicherheits- und Kontinuitätsanforderungen, Sicherheitsprinzipien, Sicherheitselemente für Betriebs- und Angriffssicherheit sowie Kontinuität je Prozess und Ressource, Risikomatrix
Sicherheits- und Kontinuitäts-elemente	Sicherheits- und Kontinuitätsrichtlinien erstellen		Sicherheits- und Kontinuitätsrichtlinien für Prozesse, RessourcenProdukte und Dienstleistungen, z. B. für Prozesse, Konformität, Datenschutz, Datensicherung, Notfallvorsorge, ...
Sicherheits- und Kontinuitätsrichtlinien, Ressourcenspezifika	Sicherheits- und Kontinuitätskonzepte entwickeln		Spezifische Konzepte

Eingangs- informationen	Aktivitäten unter Berücksichtigung von PROSim	Methoden	Ergebnisse
Sicherheits- und Kontinuitäts- konzepte	Sicherheits- und Kontinuitäts- maßnahmen ergreifen		Protokolle durchge- führter Sicherheits- und Kontinuitätsmaß- nahmen
Sicherheits- und Kontinuitäts- elemente, Prozess- und ressourcen- spezifische Le- benszyklen	Sicherheit und Kontinuität in die Lebenszyklen integrieren		Lebenszyklen mit Sicherheits- und Kon- tinuitätselementen
DO			
Ergebnisse der Planungsphase Monitoring-, Re- porting- und Cont- rolling-Anforde- rungen	Sicherheitsmanage- ment betreiben, monitoren, reporten, controllen		Protokolle, Unterlagen Messwerte, Meldungen, Reports, Controlling- Berichte
CHECK			
Prüfumfang und Rahmen- bedingungen	Sicherheits- management prüfen	HAZOP, OCTAVE [®] , Self Assess- ment, Pene- trationstest, Security- Scans, Audits, Sicherheits- studien	Prüfberichte
ACT			
Prüfberichte interne und externe Anforderungen	Sicherheits- management verbessern		Roadmap, Projektplan

17 Minimalistische Sicherheit

Die vorangegangenen Kapitel haben den systematischen und durchgängigen Aufbau des ITK-Sicherheitsmanagements anhand der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller gezeigt. Sie liefert die Grundlage, um ein unternehmensspezifisch angemessenes Sicherheitsmanagementsystem aufzubauen.

Die verschiedenen Kapitel dieses Buchs, die anfangs dargestellten Bedrohungen und die im Text genannten Ereignisse zeigen, dass Sicherheit ein methodisches Vorgehen benötigt, wie es die dreidimensionale Sicherheitspyramide liefert. Wer sich in einem kleinen Unternehmen schnell einen ersten rudimentären und minimalistischen Überblick über einige wenige wichtige Sicherheitseckpunkte verschaffen möchte, kann die folgende Checkliste nutzen. Hiermit lässt sich das prinzipielle Vorhandensein einzelner sicherheitsrelevanter Basiselemente zu prüfen, die anschließend im Detail zu verifizieren sind:

Vorhandene, umgesetzte, gelebte und geprüfte Basiselement	Erfüllt ja/nein
Zutrittsschutz, durchgängig und ausreichend granular sowie mit entsprechenden Richtlinien und Dokumentationen	
Zugangsschutz, durchgängig und ausreichend granular sowie mit entsprechenden Richtlinien und Dokumentationen	
Zugriffsschutz, durchgängig und ausreichend granular sowie mit entsprechenden Richtlinien und Dokumentationen	
ITK-Benutzerrichtlinie einschließlich E-Mail und Internet	
Richtlinien Datenschutz und Geheimhaltung	
Richtlinien ITK-Betrieb mit Einsatzverfahren für Programme und ITK-Systeme	
Datensicherung und Datensicherungsmethodik einschließlich Datenauslagerung mit Richtlinie und Dokumentationen	
Patchmanagement	
Virens Scanner, aktuell und je Arbeitsplatz/System vorhanden	
Firewall, aktuell und an allen externen Schnittstellen vorhanden	
Intrusion Detection and Prevention, aktuell	
Spam-Filter, aktuell	
Datenlöschungsrichtlinie	

Datenträgervernichtungsrichtlinie	
Notfallplanung	
Verschlüsselung	
USB-Port-Überwachung	
Lizenzmanagement	
...	

Abbildungsverzeichnis

Abb. 4.1:	ISO 27000-Reihe	31
Abb. 4.2:	IT-Sicherheitsprozess orientiert an BSI.....	33
Abb. 4.3:	BCM Lifecycle	40
Abb. 4.4:	Schutzobjektklassen	57
Abb. 4.5:	Business Continuity Management mit der Sicherheitspyramide.....	59
Abb. 4.6	Kontinuitätspyramide IV nach Dr.-Ing. Müller.....	60
Abb. 4.7	Business Continuity Pyramid IV according to Dr.-Ing. Müller	61
Abb. 4.8	Detaillierter Sicherheitsdreiklang nach Dr.-Ing. Müller	62
Abb. 4.9:	Detaillierter Risikodreiklang nach Dr.-Ing. Müller.....	64
Abb. 5.1:	Sicherheitspyramide IV nach Dr.-Ing. Müller	70
Abb. 8.1:	House of Safety, Security and Continuity (HoSSC)	120
Abb. 9.1:	Schadenklassifizierung	137
Abb. 9.2:	Kern-, Support- und Begleitprozesse im Lebenszyklus.....	155
Abb. 9.3:	Begleitprozesse (Managementdisziplinen)	162
Abb. 9.4:	ITIL® Service Life Cycle	163
Abb. 9.5:	Risikomanagementpyramide nach Dr.-Ing. Müller....	169
Abb. 9.6:	Datensicherungsmethoden	203
Abb. 9.7:	Über-Kreuz-Sicherung	208
Abb. 9.8:	Allgemeines Sicherheitsschalenmodell nach Dr.-Ing. Müller.....	212
Abb. 9.9:	Elemente des Securitymanagements gemäß Sicherheitsschalenmodell nach Dr.-Ing. Müller	216
Abb. 9.10:	Berechtigungswürfel bzw. -kubus.....	218
Abb. 9.11:	Subjekt-Subjektgruppe-Recht-Objektgruppe-Objekt- Modell	219
Abb. 9.12:	USB-Token (Prinzipdarstellung)	224
Abb. 9.13:	Taschenauthentifikator (Prinzipdarstellung)	225
Abb. 9.14:	Verschlüsselungsverfahren	238
Abb. 9.15:	Struktur einer SOAP-Nachricht (Beispiel)	249
Abb. 9.16:	Speichermedien.....	268
Abb. 9.17:	DAS, NAS, SAN.....	273
Abb. 9.18:	Firewallebenen (Prinzipdarstellung)	277
Abb. 10.1:	Notfallablauf	323
Abb. 14.1:	Sicherheitsstudie/Risikoanalyse	366
Abb. 14.2:	Sicherheitsregelkreis	373
Abb. 15.1:	Reifegradmodell nach Dr.-Ing. Müller	387
Abb. 16.1:	Sicherheitsmanagementprozess nach Dr.-Ing. Müller	393

Markenverzeichnis

Die folgenden Angaben erfolgen ohne Gewähr und ohne Haftung. Es gelten die entsprechenden Schutzbestimmungen und -rechte in ihrer jeweils aktuellen Fassung.

CERT® und CERT Coordination Center® (CERT®/CC) sind eingetragene Marken der Carnegie Mellon University.

Certified Information Security Manager™, CISM™, Certified Information Security Auditor™ und CISA™ sind Marken der Information Systems Audit and Control Association®, Inc. (ISACA®).

CMM®, CMMI®, Capability Maturity Model®, Capability Maturity Model Integration® sind eingetragene Marken der Carnegie Mellon University.

COBIT® ist eine eingetragene Marke der Information Systems Audit and Control Association® und des IT Governance Institute®.

Honeynet Project® ist eine eingetragene Marke des Honeynet Project, einer NOT-FOR-PROFIT CORPORATION.

IDEA™ ist eine Marke der Ascom Systec Ltd.

Information Systems Audit and Control Association® und ISACA® sind eingetragene Marken der Information Systems Audit and Control Association®.

IT Governance Institute® und ITGI® sind eingetragene Marken der Information Systems Audit and Control Association.

ITIL® ist eine eingetragene Marke des Office of Government Commerce (OGC).

Kerberos™ ist eine Marke des Massachusetts Institute of Technology (MIT).

Lotus Notes® ist eine eingetragene Marke der International Business Machines Corporation (IBM).

Microsoft®, Windows®, NT® sind eingetragene Marken der Microsoft Corporation.

Novell ist eine eingetragene Marke der Novell Inc., USA.

OGFSM, Open Grid ForumSM, Grid ForumSM, OGSA™ und Open Grid Services Architecture sind Marken des Open Grid Forums.

RC5™ ist eine Marke der RSA Security Inc.

SAP® ist eine eingetragene Marke der SAP AG.

Stratus® und Continuous Processing® sind eingetragene Marken von Stratus Technologies Bermuda Ltd.

UNIX® ist eine eingetragene Marke der „The Open Group“.

Wi-Fi® ist eine eingetragene Marke der Wi-Fi Alliance.

zSeries® ist eine eingetragene Marke der International Business Machines Corporation (IBM).

Verzeichnis über Gesetze, Vorschriften, Standards, Normen, Practices

Die folgenden Unterkapitel nennen einige Gesetze, Ausführungsbestimmungen, Grundsätze, Vorschriften, Standards, Normen und Practices, die im Zusammenhang mit dem Sicherheits-, Kontinuitäts- und Risikomanagement eine Rolle spielen. Diese sind teils branchenübergreifend und teils branchenspezifisch. Sie behandeln z. B. Themen wie Sorgfaltspflicht der Vorstandsmitglieder, Überwachungssystem, Risiken, Notfallplanung, Datenschutz und Ordnungsmäßigkeit.

11. Sicherheitsstudie der <kes> 2006 [90]

Aufgrund der in [90] erhobenen Informationen ist das Bundesdatenschutzgesetz (BDSG) bei den Teilnehmern an der Sicherheitsstudie am bekanntesten und für rund 90 % der Befragten auch relevant. Demgegenüber kennen das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) nicht ganz 70 % der Befragten. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist 70 % der Befragten bekannt. Wenngleich der Bekanntheitsgrad im Vergleich zu früheren Studien zugenommen hat, sind diese Zahlen insofern noch etwas ernüchternd, als die Vorschriften des Teledienste- und Telekommunikationsgesetzes für die Protokollierung auf Firewalls, Web- und Mail-Servern [91] eine hohe Bedeutung besitzen und das KonTraG, das seinen Niederschlag im Aktiengesetz gefunden hat, die Einrichtung eines Risikomanagementsystems fordert.



Deutsche Gesetze und Verordnungen

Abgabenordnung	<i>AO</i>
Aktiengesetz	<i>AktG</i>
Bundesdatenschutzgesetz	<i>BDSG</i>
GmbH-Gesetz	<i>GmbHG</i>
Geldwäschegesetz	<i>GwG</i>
Handelsgesetzbuch	<i>HGB</i>
Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste	<i>luKDG</i>
• Artikel 1: Teledienstegesetz (TDG)	
• Artikel 2: Teledienstedatenschutzgesetz (TDDSG)	
• Artikel 3: Signaturgesetz (SigG)	

<i>KAGG</i>	Gesetz über Kapitalanlagegesellschaften (Kapitalanlagegesellschaftengesetz)
<i>KonTraG</i>	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
<i>KWG</i>	Kreditwesengesetz
<i>SGB</i>	Sozialgesetzbuch
<i>SigG</i>	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
<i>SigV</i>	Verordnung zur elektronischen Signatur (Signaturverordnung)
<i>TDDSG</i>	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz)
<i>TDG</i>	Gesetz über die Nutzung von Telediensten (Teledienstegesetz)
<i>TDSV</i>	Telekommunikations-Datenschutzverordnung
<i>TKG</i>	Telekommunikationsgesetz
<i>TKÜV</i>	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung)
<i>TMG</i>	Telemediengesetz
<i>UrhG</i>	Urheberrechtsgesetz
<i>WpHG</i>	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz)

Österreichische Gesetze und Verordnungen

<i>BWG</i>	Bankwesengesetz
<i>DSG 2000</i>	Datenschutzgesetz 2000
<i>InfoSiG</i>	Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz)
<i>InfoSiV</i>	Verordnung der Bundesregierung über die Informationssicherheit (Informationssicherheitsverordnung)

Schweizer Gesetze, Verordnungen und Richtlinien

<i>BankG</i>	Bundesgesetz über die Banken und Sparkassen (Bankengesetz)
<i>BankV</i>	Verordnung über die Banken und Sparkassen (Bankenverordnung)
<i>DSG</i>	Bundesgesetz über den Datenschutz (Datenschutzgesetz)

Interne Revision (Inspektorat), Rundschreiben der Eidgenössischen Bankenkommission, 14. Dezember 1995	<i>EBK-RS 95/1</i>
Richtlinie zur Bekämpfung und Verhinderung der Geldwäscherei, Rundschreiben der Eidgenössischen Bankenkommission, 26. März 1998	<i>EBK-RS 98/1</i>
Auslagerung von Geschäftsbereichen (Outsourcing), Rundschreiben der Eidgenössischen Bankenkommission, 26. August 1999	<i>EBK-RS 99/2</i>
Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung)	<i>GeBüV</i>
Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz)	<i>GwG</i>
Verordnung der Eidgenössischen Bankenkommission zur Verhinderung von Geldwäscherei (EBK Geldwäschereiverordnung)	<i>GwV EBK</i>
Verordnung zum Bundesgesetz über den Datenschutz	<i>VD SG</i>

Britische Gesetze, Verordnungen und Richtlinien

Freedom of Information Act (FoIA) 2000	<i>FoIA</i>

Europäische Richtlinien

Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 2000/520/EG	<i>Entscheidung 2000/520/EG</i>
Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG	<i>Entscheidung 2002/16/EG</i>
Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	<i>Richtlinie 95/46/EG</i>
Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)	<i>Richtlinie 2002/58/EG</i>
Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäfts-	<i>Richtlinie 2000/31/EG</i>

	verkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“)
<i>Richtlinie 2006/43/EG EuroSOX</i>	Richtlinie 2006/43/EG des europäischen Parlaments und der Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen(EuroSOX)
	European Communities: Guidelines on best practices for using electronic information, 1997
<i>PIC/S PI 011-2</i>	Good Practices for Computerised Systems in regulated „GxP“ Environments, PI 011-2, PIC/S, Juli 2004

US-amerikanische Gesetze, Verordnungen und Richtlinien

<i>21 CFR Part 11</i>	Electronic Records; Electronic Signatures, Code of Federal Regulations; Title 21, Part 11
<i>COPPA</i>	Children’s Online Privacy Protection Act
<i>DPPA</i>	Drivers Privacy Protection Act
	Electronic Communications Privacy Act
<i>FDIC, Managing Multiple Service Providers</i>	Technology Outsourcing, Techniques for Managing Multiple Service Providers
<i>FDIC, Selecting a Service Provider</i>	Technology Outsourcing, Effective Practices for Selecting a Service Provider
<i>FERPA</i>	Family Educational Rights and Privacy Act
<i>FFIEC, BCP</i>	IT Examination Handbook, Business Continuity Planning, März 2003
<i>FFIEC, OT</i>	IT Examination Handbook, Outsourcing Technology Services, Juni 2004
<i>FFIEC, TSP</i>	IT Examination Handbook, Supervision of Technology Service Providers (TSP), März 2003
<i>FISMA</i>	Federal Information Security Management Act of 2002
<i>GLBA</i>	Gramm-Leach-Bliley Act
	Privacy Act
<i>SOX</i>	Sarbanes-Oxley Act

Ausführungsbestimmungen, Grundsätze, Vorschriften

Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen	<i>Basel II</i>
Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen	<i>GDPdU</i>
Grundsätze ordnungsmäßiger Buchführung	<i>GoB</i>
Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme. Die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) hat am 21. Juli 2004 die Projektgruppe 3.4.1 gebildet, die sich die Überarbeitung und Aktualisierung der GoBS zum Ziel gesetzt hat.	<i>GoBS</i>
Grundsätze für eine ordnungsmäßige Datenverarbeitung [92]	<i>GoDV</i>
Grundsätze ordnungsmäßiger Speicherbuchführung (neu gefasst in GoBS)	<i>GoS</i>
Abschlußprüfung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Stand: 24.09.2002	<i>IDW PS 330</i>
Erteilung und Verwendung von Softwarebescheinigungen (IDW), Stand: 25.06.1999	<i>IDW PS 880</i>
Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), 24.09.2002	<i>IDW RS FAIT 1</i>
Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), 24.09.2003	<i>IDW RS FAIT 2</i>
Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren, Verlautbarung des Instituts der Wirtschaftsprüfer (IDW), Fachausschuss für Informationstechnologie (FAIT), Stand: 11.07.2006	<i>IDW RS FAIT 3</i>
Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – IuK-Mindestanforderungen	<i>MaIuK</i>
Mindestanforderungen an das Risikomanagement, BaFin	<i>MaRisk</i>
Grenzüberschreitende Datenfernverarbeitung im Bankbuchführungswesen, Bundesaufsichtsamt für das Kreditwesen, 10/1992	

Standards, Normen, Leitlinien und Rundschreiben

<i>ANSI/IEEE Std.</i> 829-1983	Standard for Software Test Documentation
<i>ANSI/IEEE Std.</i> 1008-1987	Standard for Software Unit Test
<i>ANSI/IEEE Std.</i> 1012-1986	Standard for Software Verification and Validation Plans
<i>BAKred,</i> <i>Rundschreiben</i> 10/1992	Grenzüberschreitende Datenfernverarbeitung im Bankbuchführungswesen, Bundesaufsichtsamt für das Kreditwesen
<i>BAKred,</i> <i>Rundschreiben</i> 11/2001	Auslagerung von Bereichen auf ein anderes Unternehmen gemäß §25a Abs. 2 KWG, Bundesaufsichtsamt für das Kreditwesen, Rundschreiben 11/2001, I3 – 272A – 2/98
<i>Baseler Ausschuss, Risk Management Principles,</i> <i>Mai 2001</i>	Risk Management Principles for Electronic Banking, Baseler Ausschuss
<i>Baseler Ausschuss, Sound Practices,</i> <i>Februar 2003</i>	Sound Practices for the Management and Supervision of Operational Risk, Baseler Ausschuss
<i>BS 25999-1:2006</i>	Code of practice for business continuity management. Diese britische Norm ersetzt PAS 56:2003.
<i>BS 25999-2</i>	Business Continuity Management, Part 2: Specification. Dieser britische Standard liegt im Entwurf vor und soll im Jahr 2007 verabschiedet werden.
<i>BSI-Standard</i> 100-1:2005	Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Dezember 2005
<i>BSI-Standard</i> 100-2:2005	IT-Grundschutz-Vorgehensweise, Version 1.0, Dezember 2005
<i>BSI-Standard</i> 100-3:2005	Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.0, Dezember 2005

Common Criteria, Version 3.1, September 2006	CC, V 3.1
Common Methodology for Information Security Evaluation, Version 3.1, September 2006	CEM, V 3.1
Capability Maturity Model® (Vorgänger vom CMMI®)	CMM®
Capability Maturity Model Integration®	CMMI®
Control Objectives for Information and related Technology	COBIT®
COTS Security Protection Profile – Operating Systems	CSPP-OS
Qualitätsmanagementsysteme – Anforderungen	DIN EN ISO 9001
Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene – Teil 9: Sicherheitsschlüssel- und Zertifikatsverwaltung	DIN ISO 9735-9
Qualitätsmanagement – Leitfaden für Konfigurationsmanagement	DIN ISO 10007
Medizinische Informatik – Sichere Nutzeridentifikation im Gesundheitswesen – Management und Sicherheit für die Authentifizierung durch Passwörter, 2004-01	DIN EN 12251
EDIFACT – Anwendungsregeln – Teil 15: Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten	DIN 16560-15
Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Teil 4: Regeln zur Auszeichnung von UN/EDIFACT-Übertragungsdateien mit der eXtensible Markup Language (XML) unter Einsatz von Document Type Definitions (DTD's)	DIN 16557-4
Büro- und Datentechnik – Vernichtung von Informationsträgern – Teil 1: Anforderungen und Prüfungen an Maschinen und Einrichtungen	DIN 32757-1
Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) {RAMS = Reliability, Availability, Maintainability, Safety}	DIN EN 50126
Unterbrechungsfreie Stromversorgungssysteme (USV) – Teil 3: Methoden zur Festlegung der Leistungs- und Prüfungsanforderungen (IEC 62040-3)	DIN EN 62040-3
Wertbehälter – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand – Teil 1: Datensicherungsschränke	EN 1047-1
Wertbehälter – Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand – Teil 2: Datensicherungsräume und Datensicherungscontainer	EN 1047-2

<i>FinTS</i>	Financial Transaction Services
<i>GAMP</i>	The Good Automated Manufacturing Practice (GAMP) – Guide for Validation of Automated Systems in Pharmaceutical Manufacture
<i>GERM</i>	Good Electronic Records Management
<i>HBCI</i>	Home Banking Computer Interface
<i>ISO/IEC 2382-8</i>	Informationstechnik – Begriffe – Teil 8: Sicherheit, 1998-11
<i>ISO/IEC 10118-1,2,3,4</i>	Information technology – Security techniques – Hash-functions • Part 1: General, 2000 • Part 2: Hash-functions using an n-bit block cipher, 2000 • Part 3: Dedicated hash-functions, 2004 • Part 4: Hash-functions using modular arithmetic, 1998
<i>ISO/IEC 13335-1</i>	Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 11/2004, Deutsche Fassung 11/2006
<i>ISO/IEC 13335-2</i>	Information technology – Security techniques – Management of information and communications technology security – Part 2: Techniques for information and communications technology security risk management. Diese Norm befindet sich in Vorbereitung. In sie sollen die früheren Technical Reports ISO/IEC TR 13335-3, Techniques for the management of Information Technology security, und ISO/IEC TR 13335-4, Selection of safeguards, einfließen
<i>ISO/IEC TR 13335-3</i>	Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security, 1998 (befindet sich in Überarbeitung)
<i>ISO/IEC TR 13335-4</i>	Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards, 2000 (befindet sich in Überarbeitung)
<i>ISO/IEC TR 13335-5</i>	Information technology – Security techniques – Guidelines for the management of Information Technology security – Part 5: Management guidance on network security, 2001 (befindet sich in Überarbeitung und soll in ISO/IEC 18028-1 einfließen)
<i>ISO/IEC 13888 –1,2,3</i>	Information technology (Informationstechnik) – Security techniques (Sicherheitsverfahren) – Non-repudiation (Nicht-Abstreitbarkeit) • Part 1: General (Allgemeines Modell), 2004 • Part 2: Mechanisms using symmetric techniques (Mechanismen auf Basis von symmetrischen Techniken), 1998-04

- Part 3: Mechanisms using asymmetric techniques (Mechanismen auf Basis von asymmetrischen Techniken), 1997-1.2
- Information technology (Informationstechnik) – Security techniques (Sicherheitsverfahren) – Digital signatures with appendix (Digitale Signaturen mit Anhang) *ISO/IEC 14888-1,2,3*
- Part 1: General, 1998
- Part 2: Identity-based mechanisms, 1999, in Überarbeitung zu „Integer factorization based mechanisms“
- Part 3: Discrete logarithm based mechanisms, 2006.
- Erweiterbare Auszeichnungssprache für das elektronische Geschäftswesen (eXML), Teil 1 bis 4, Vornorm *ISO/TS 15000*
- Informationstechnik – Bewertung von Software-Prozessen *ISO/IEC TR 15504-1 ... 5*
- Information technology – Security techniques – Evaluation criteria for IT security s. a. Common Criteria *ISO/IEC 15408-1,2,3*
- Part 1: Introduction and general model, 2005
- Part 2: Security functional requirements, 2005
- Part 3: Security assurance requirements, 2005.
- Im September 2006 verabschiedete die Staatengemeinschaft die Common Criteria Version 3.1 und legte sie der ISO zur Standardisierung vor (s. a. ISO/IEC FCD 15408-2,3)
- Information technology (Informationstechnik) – Security techniques (Sicherheitsverfahren) – A framework for IT security assurance (Ein Rahmenwerk zur Qualitätssicherung der IT-Sicherheit) *ISO/IEC TR 15443-1,2,3*
- Part 1: Overview and framework, 2005
- Part 2: Assurance methods, 2005
- Part 3: Analysis of assurance methods, Status: CD.
- Information technology (Informationstechnik) – Security techniques (Sicherheitsverfahren) – Guide for the production of Protection Profiles and Security Targets *ISO/IEC TR 15446:2004*
- Information and documentation: Records management *ISO 15489-1, ISO 15489-2TR*
- Part 1: General
- Part 2: Guidelines.
- Information technology (Informationstechnik) – Security techniques (Sicherheitsverfahren) – Cryptographic techniques based on elliptic curves *ISO/IEC 15946-1,2,3,4*
- Part 1: General, 2002
- Part 2: Digital signatures, 2002

	• Part 3: Key establishment, 2002 • Part 4: Digital signatures giving message recovery, 2004.
<i>ISO/IEC TR 15947</i>	Information technology – Security techniques – IT intrusion detection framework, 2002-10
<i>ISO/IEC 17799</i>	Information technology – Security techniques – Code of practice for information security management (Die ISO/IEC 17799:2000 ist hervorgegangen aus dem British Standard BS 7799-1:2000. Im Jahr 2005 ist die überarbeitete Norm ISO/IEC 17799:2005 erschienen.)
<i>ISO/IEC 18028-1,2,3,4,5</i>	Information technology – Security techniques – IT network security (Die Normenreihe ISO/IEC 18028 stellt die Verbindung her zwischen den allgemeinen Richtlinien für das IT-Sicherheitsmanagement der ISO/IEC 13335 und der konkreten technischen Implementierung der Netz-Sicherheit) • Part 1: Network security management, 2006 • Part 2: Network security architecture, 2006 • Part 3: Securing communications between networks using security gateways, 2005 • Part 4: Securing remote access, 2005 • Part 5: Securing communications across networks using virtual private networks, 2006.
<i>ISO/IEC TR 18044:2004</i>	Information Technology – Security Techniques – Information security incident management
<i>ISO/IEC 20000-1,2:2005</i>	Information technology – Service management • Part 1: Specification (basiert auf dem Standard BS 15000 und löst ihn ab) • Part 2: Code of practice (basiert auf dem Standard BS 15000-2 und löst ihn ab).
<i>ISO/IEC 21827:2002</i>	Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM [®])
<i>ISO/IEC 21000-5:2004</i>	Information technology – Multimedia framework (MPEG-21) – Part 5: Rights Expression Language
<i>ISO/IEC PRF TR 24731</i>	Information technology – Programming languages, their environments and system software interfaces – Extensions to the C library – Part 1: Bounds-checking interfaces
<i>ISO/IEC FCD 24759</i>	Information technology – Security techniques – Requirements for Cryptographic Models
<i>ISO/IEC NP 24760</i>	Information technology – Security techniques – A Framework for Identity Management

Information technology – Authentication context of biometrics (ACBio)	ISO/IEC FCD 24761
Guidelines for Information and Communication Technology Disaster Recovery Scenario	ISO/IEC FCD 24762
Information technology – Generic cabling for data-centres	ISO/IEC NP 24764
Information technology – Security techniques – Information security management systems – Overview and vocabulary	ISO/IEC FCD 27000
Information technology – Security techniques – Information security management systems – Requirements	ISO/IEC 27001:2005
Information technology – Security techniques – Code of practice for information security management. Standard, der seit Juli 2007 die bisherige ISO 17799:2005 unter dieser neuen Nummer weiterführt.	ISO/IEC 27002:2005
Angedachter Standard, der zusätzliche Implementierungsrichtlinien und Teile der ISO 13335 (technische Aspekte) enthalten soll [93]	ISO/IEC 27003
Information technology – Information security management measurements. Standard, der Kontrollelemente (metrics and measurements) zur IT-Sicherheit enthalten soll [93]	ISO/IEC CD 27004
Information technology – Information security risk management. Standard, der Richtlinien zum Risikomanagement enthalten soll [93]	ISO/IEC FCD 27005
Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	ISO/IEC 27006:2007
Angedachter Standard, der z. B. unter dieser Nummer den Standard X.1051 ITU-T integrieren könnte. Dieser würde dann die ISO 27002 um zusätzliche Telekommunikationsanforderungen der International Telecommunications Union (ITU) erweitern [93]	ISO/IEC 27051, angedacht
Health informatics – Security management in health using ISO/IEC 17799	ISO/DIS 27799
Information technology – Basic Profile Version 1.1	ISO/IEC DIS 29361
Information technology – Attachments Profile Version 1.	ISO/IEC DIS 29362
Information technology – Simple SOAP Binding Profile Version 1.0	ISO/IEC DIS 29363

<i>ISO/IEC DIS 29382</i>	Corporate Governance of Information and Communication Technology
<i>IT-GSHB</i>	IT-Grundschriftzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieses teilt sich seit Ende 2005 auf in die Grundschriftz-Vorgehensweise und die IT-Grundschriftzkataloge (IT-GSK), die sich ihrerseits aus Gefährdungs- und Maßnahmenkatalogen zusammensetzen.
<i>ITIL®</i>	IT Infrastructure Library des Office of Government Commerce (OGC)
<i>ITSEC</i>	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Bundesanzeiger, Stand: Juni 1991
<i>NIST: IT Security Assessment Framework</i>	Federal Information Technology Security Assessment Framework, NIST
<i>NIST SP800-16</i>	Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998
<i>NIST SP800-26</i>	Security Self-Assessment Guide for Information Technology Systems, NIST, November 2001
<i>NIST SP800-27</i>	Engineering Principles for IT Security, NIST, Juni 2001
<i>NIST SP800-30</i>	Risk Management Guide for Information Technology Systems, NIST, Juli 2002
<i>NIST SP800-36</i>	Guide to Selecting Information Technology Security Products, NIST, Oktober 2003
<i>NIST SP800-41</i>	Guidelines on Firewalls and Firewall Policy, NIST, Januar 2002
<i>NIST SP800-94</i>	Guide to Intrusion Detection and Prevention Systems (IDPS), NIST, Februar 2007
<i>OASIS™ AVDL, 2004</i>	Application Vulnerability Description Language v1.0, OASIS™, Mai 2004
<i>OASIS™ CAP, 2005</i>	Common Alerting Protocol v1.1, OASIS™, Oktober 2005
<i>OASIS™ DSS, 2007</i>	Digital Signature Service Core Protocols, Elements, and Bindings 1.0, OASIS™, April 2007
<i>OASIS™ DSS: AdES, 2007</i>	Advanced Electronic Signature Profiles of the OASIS Digital Signature Service 1.0, OASIS™, 11. April 2007
<i>OASIS™ DSS: Code-Signing, 2007</i>	Abstract Code-Signing Profile of the OASIS Digital Signature Services 1.0, OASIS™, 11. April 2007

Electronic PostMark (EPM) Profile of the OASIS Digital Signature Service 1.0, OASIS™, 11. April 2007	<i>OASIS™ DSS: EPM, 2007</i>
XML Timestamping Profile of the OASIS Digital Signature Services 1.0, OASIS™, 11. April 2007	<i>OASIS™ DSS: Timestamping, 2007</i>
Emergency Data Exchange Language (EDXL), Distribution Element, v. 1.0, OASIS™, März 2006	<i>OASIS™ EDXL-DE, 2006</i>
Security Assertion Markup Language (SAML) 2.0, OASIS™, 15. März 2005	<i>OASIS™ SAML, 2005</i>
German Signature Law Profile of the OASIS Digital Signature Service 1.0, OASIS™, 11. April 2007	<i>OASIS™ SigG, 2006</i>
Reference Model for Service Oriented Architecture 1.0, OASIS™, Oktober 2006	<i>OASIS™ SOA, 2006</i>
Service Provisioning Markup Language, Version 2, OASIS™, April 2006	<i>OASIS™ SPML, 2006</i>
Universal Description, Discovery and Integration (UDDI) , OASIS™	<i>OASIS™ UDDI</i>
Web Services Security: Kerberos Token Profile 1.1, OASIS™, Februar 2006	<i>OASIS™ WSS: Kerberos, 2006</i>
Web Services Security: Rights Expression Language (REL) Token Profile 1.0, OASIS™, 19. Dezember 2004	<i>OASIS™ WSS: REL, 2004</i>
Web Services Security: SAML Token Profile 1.1, OASIS™, 1. Februar 2006	<i>OASIS™ WSS: SAML, 2006</i>
Web Services Security: SOAP Message Security 1.1, OASIS™, 1. Februar 2006	<i>OASIS™ WSS: SOAP, 2006</i>
Web Services Security: Username Token Profile 1.1, OASIS™-, 1. Februar 2006	<i>OASIS™ WSS: Username, 2006</i>
Web Services Security: X.509 Certificate Token Profile 1.1, OASIS™, Februar 2006	<i>OASIS™ WSS: X.509, 2006</i>
Web Services SecureConversation 1.3, OASIS™, 1. März 2007	<i>OASIS™ WS-Secure-Conversation, 2007</i>
Web Services Trust 1.3, OASIS™ , 19. März 2007	<i>OASIS™ WS-Trust, 2007</i>

<i>OASIS™ XACML, 2005</i>	eXtensible Access Control Markup Language (XACML) 2.0, OASIS™, Februar 2005
<i>OGSA™, 2006</i>	Open Grid Services Architecture™ (OGSA™) 1.5, OGF, 24. Juli 2006
<i>OGSA™ Basic Security Profile, 2006</i>	OGSA™ Basic Security Profile 1.0 – Core, OGF, 10. November 2006
<i>OGSA™ Security Profile, 2007</i>	OGSA™ Security Profile 1.0 – Secure Channel, OGF, 22. Januar 2007
<i>OGSA™ SAML, 2006</i>	Use of SAML for OGSi Authorization, Status „experimentell“, OGF, 26. März 2006
<i>PAS 77:2006</i>	IT Service Continuity Management – Code of Practice
<i>SPICE</i>	Software Process Improvement and Capability dEtermination, s. a. ISO/IEC TR 15504
<i>SSE-CMM®</i>	Information technology – Systems Security Engineering – Capability Maturity Model (ISO/IEC 21827:2002)
<i>The Joint Forum, Outsourcing, August 2004</i>	Outsourcing in Financial Services, Consultative document, The Joint Forum, Baseler Ausschuss
<i>The Joint Forum, Business Continuity, December 2005</i>	High-level principles for business continuity, Consultative document, The Joint Forum, Basel Committee on Banking Supervision
<i>W3C® SOAP, 2007</i>	Simple Object Access Protocol (SOAP) 1.2, 2. Ausgabe, W3C®, 27. April 2007
<i>W3C® WSDL, 2007</i>	Web Services Description Language (WSDL) 2.0, W3C®, Mai 2007, vorgelegt zur abschließenden Freigabe
<i>W3C® XKMS, 2005</i>	XML Key Management Specification (XKMS) 2.0, W3C®, 28. Juni 2005
<i>X.1051</i>	Recommendation X.1051 – Information Security Management System – Requirements for Telecommunications (ISMS-T). In dieser Empfehlung sind die Anforderungen an den Aufbau, die Implementierung, den Betrieb, das Monitoring, die Prüfung, die Wartung und die Verbesserung eines dokumentierten ISMS für Telekommunikationsunternehmen beschrieben.

Literatur- und Quellenverzeichnis

- [1] Müller, Klaus-Rainer: IT-Sicherheitsmanagement und die Rolle der Unternehmensberater, Datensicherheitstage, 5. Oktober 1995
- [2] <kes>/Microsoft-Sicherheitsstudie 2006, Lagebericht zur Informations-Sicherheit, Teil 1, <kes>, 4/2006, S. 24ff.
- [3] Eagle Rock Alliance Ltd., Contingency Planning Research, Online Survey Results, 2001 Cost of Downtime
- [4] Müller, Klaus-Rainer: IT-Sicherheit mit System, VIEWEG, Juli 2003
- [5] Müller, Klaus-Rainer: Unternehmensberater – Ungeliebte Zaungäste?, KES, 2/1996 vom Mai 1996, S. 6ff.
- [6] Müller, Klaus-Rainer: Risiken vermeiden, Business Computing, 7/1996, S. 46ff.
- [7] Müller, Klaus-Rainer: Sicherheits- und Qualitätsmanagement – zwei Seiten einer Medaille?, KES, 3/1996, S. 111ff.
- [8] Müller, Klaus-Rainer: Genormte Sicherheit – Gesetze, Standards, Practices im Überblick, ix, 1/2007, S. 95ff.
- [9] Müller, Klaus-Rainer: Lebenszyklus- und prozessimmanente IT-Sicherheit, <kes>, 3/2004, S. 72ff.
- [10] IT Governance Institute®: COBIT® 4.0, 2005
- [11] Kaplan, Robert S., Norton, David P.: Balanced Scorecard, Schäffer-Poeschel, 1997
- [12] Anderson, Ross: Security Engineering, Wiley, 2001
- [13] Müller, Klaus-Rainer: Risikoanalyse diktiert die Handlung, Computerzeitung, 38/2004, S. 17
- [14] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Bundesanzeiger, Stand: Juni 1991
- [15] ISO 15408-1, 2, 3 Informationstechnologie – IT-Sicherheitsverfahren, bzw. Common Criteria, Version 2.1, Teil 1, 2, 3
- [16] Common Criteria for Information Technology Security Evaluation, Version 2.3, Teil 1, 2, 3, August 2005
- [17] Brockhaus, die Enzyklopädie in 24 Bänden, Studienausgabe, Band 18, Brockhaus, 2001
- [18] Baseler Ausschuss für Bankenaufsicht: Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderungen, Überarbeitete Rahmenvereinbarung, Übersetzung der Deutschen Bundesbank, Juni 2004
- [19] Von der Crone, Hans Caspar und Roth, Katja: Der Sarbanes-Oxley Act und seine extraterritoriale Bedeutung, AJP/PJA, 2/2003, S. 131 ff.
- [20] Institut der Wirtschaftsprüfer: Rechnungslegung und Prüfung bei Einsatz von Informationstechnologie, Die neuen IDW-Verlautbarungen, IDW-Verlag GmbH, 2002

- [21] Institut der Wirtschaftsprüfer: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3), 11. Juli 2006
- [22] Masing, Walter (Hrsg.): Handbuch Qualitätsmanagement, 3. Auflage, 1994
- [23] Suzuki, Kiyoshi: Die ungenutzten Potentiale, Carl Hanser Verlag, 1994
- [24] DeMarco, Tom: Structured Analysis and System Specification, New York, Yourdon Press, 1978
- [25] OASIS™: Reference Model for Service Oriented Architecture 1.0, OASIS Standard, 12.10.2006
- [26] Office of Government Commerce: ITIL Refresh: Scope and development plan, June 2006
- [27] Jürgen Dierlamm: Neues – und Offizielles – über ITIL Version 3, itService Management, Heft 3, April 2007
- [28] www.itil.org/de, eingesehen am 1. Juni 2007
- [29] Kamiske, Gerd F. und Brauer, Jörg-Peter: Qualitätsmanagement von A bis Z, Carl Hanser Verlag, 1993
- [30] Bundesaufsichtsamt für das Kreditwesen: Auslagerung von Bereichen auf eine anderes Unternehmen gemäß §25a, Abs. 2 KWG, Rundschreiben 11/2001, Bundesaufsichtsamt für das Kreditwesen
- [31] Müller, Klaus-Rainer: In oder Out? – Sourcing mit System, geldinstitute, 3/2004, S. 32ff.
- [32] Datalink Corporation: Storage Area Networks & Return on Investment, White Paper, ohne Datum
- [33] Sherman, Larry: Stratus® Continuous Processing® Technology®, 2003
- [34] Basel Committee on Banking Supervision: Sound Practices for the Management and Supervision of Operational Risk, February 2003
- [35] Müller, Klaus-Rainer: Sicherheitsaspekte mobiler Datenkommunikation – Risikoanalyse, Schutzbedarf, Sicherheitspyramide, Schutzmaßnahmen; Seminar der ACG GmbH zur Mobilen Datenkommunikation – Chancen und Risiken, Konferenzzentrum des ZDF, 8. Oktober 1996
- [36] Medvinsky, Sasha und Lalwaney, Poornima: Kerberos V Authentication Mode for Uninitialized Clients, 29. August 2000, www.ietf.org/proceedings/00jul/SLIDES/dhckkerberos/sld000.htm
- [37] Cheswick, William R. und Bellovin, Steven M.: Firewalls und Sicherheit im Internet, Addison-Wesley, 1996
- [38] Liberty Alliance Project: Business Benefits of Federated Identity, April 2003
- [39] Liberty Alliance Project: Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, März 2003

- [40] Liberty Alliance Project: Liberty ID-FF Architecture Overview, Version 1.2
- [41] Liberty Alliance Project: Privacy and Security Best Practices, Version 2.0, 12. November, 2003
- [42] Liberty Alliance Project: Liberty ID-WSF Security and Privacy Overview, Version 1.0
- [43] Liberty Alliance Project: Liberty ID-WSF – Web Services Framework Overview, Version 2.0
- [44] Liberty Alliance Project: Liberty ID-SIS Personal Profile Service Specification, Version 1.1
- [45] Federal Information Processing Standards Publication 197 (FIPS PUBS 197): Advanced Encryption Standard (AES), 26. November 2001
- [46] Baldwin, R. und Rivest, R.: RFC 2040, The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithm, Oktober 1996, Category: Informational
- [47] Callas, J., Donnerhake, L., Finney, H., Thayer, R.: RFC 2440, OpenPGP Message Format, November 1998
- [48] Gutmann, Peter: Secure Deletion of Data from Magnetic and Solid-State Memory, 6. USENIX Security Symposium Proceedings, 22.-25.Juli 1996
- [49] Sikora, Axel: Netzwerk-Sicherheit, in IT-Security, tecCHANNEL compact, 2/2003, S. 100ff.
- [50] Farmer, Dan und Venema, Wietse: The Coroner's Toolkit, www.porcupine.org/forensics/tct.html, Stand 20.3.2005
- [51] Dillaway, Blair, Hogg, Jason: Security Policy Assertion Language (SecPAL) Specification 1.0, 15. Februar 2007
- [52] Müller, Klaus-Rainer: Der Architekturtrichter, *geldinstitute*, 6/2002, S. 44ff.
- [53] European Communities: Guidelines on best practices for using electronic information, 1997
- [54] Van Bogart, John W. C.: Media Stability, National Media Laboratory, 1996
- [55] Die 21 Stufen zur Datensicherheit, *Informationweek*, 13/2000
- [56] Storage Networking Industry Association (SNIA): Common RAID Disk Data Format Specification, revision 01.00.00, Draft for Membership Vote, 6. Juli 2004
- [57] RAID Advisory Board: RAB Classification For Disk Systems, 19. November 1997, www.raid-advisory.com/classinfo.html
- [58] Auspex Systems: A Storage Architecture Guide, White Paper
- [59] IDC: Worldwide Disk Storage Systems 2007–2011 Forecast, Mai 2007
- [60] Török, Elmar: Entwicklung der Speicherkomponenten, *lanline*, 2/2003, S. 42ff.
- [61] Courtney, Tim: JBOD, MBOD, SBOD – der kleine Unterschied, *LANline*, 5/2007, S. 56ff.

- [62] Storage Networking Industry Association (SNIA): Storage Management Initiative Specification, 1.1.1 Revision 1, 5. Juni 2007
- [63] J. Satran, K. Meth, IBM, C. Sapuntzakis, Cisco Systems, M. Chadalapaka, Hewlett-Packard Co., E. Zeidner, IBM: Internet Small Computer Systems Interface (iSCSI), RFC 3720, April 2004
- [64] M. Rajagopal, E. Rodriguez, R. Weber: Fibre Channel over TCP/IP (FCIP), RFC 3821, Juli 2004
- [65] Lange, Christoph: Trends im Speicherbereich, LANline, 5/2007, S. 52ff.
- [66] Dembeck, Michael: Firewalls – Gegen virtuelle Katastrophen, KES, 4/1999, S. 23ff.
- [67] Kyas, Othmar und a Campo, Markus: IT-Crackdown, mitp-Verlag, 2002
- [68] Schneier, Bruce: Secrets & Lies, dpunkt.verlag, 2001
- [69] Lipinski, Klaus: Lexikon der Datenkommunikation, DATACOM Buchverlag GmbH, 3. Auflage, 1995
- [70] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge, Dezember 2005
- [71] Wack, John und Cutler, Ken sowie Pole, Jamie: Guidelines on Firewalls and Firewall Policy, National Institute of Standards and Technology (NIST), NIST Special Publication 800-41, Januar 2002
- [72] Wurm, Andreas: Überwachungssysteme in Netzwerken, tecCHANNEL compact, 4/5/6/2007, S. 31ff.
- [73] <http://honeynet.org/misc/project.html>, Stand 20.3.2005
- [74] LaBrea: "Sticky" Honeypot and IDS, <http://labrea.sourceforge.net/labrea-info.html>, eingesehen am 16. Juni 2007
- [75] Müller, Klaus-Rainer: Biometrie – Verfahren, Trends, Chancen und Risiken, hakin9, 2/2007, S. 50ff.
- [76] Bundesamt für Sicherheit in der Informationstechnik: Hinweise zur räumlichen Entfernung zwischen redundanten Rechenzentren, datumsfreie pdf-Unterlage, eingesehen am 5. Oktober 2006
- [77] The Federal Reserve Board: Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations, September 1997
- [78] Müller, Klaus-Rainer: Notfallübung – Geplant, geübt, für gut befunden, IT magazin, Heft 1/2007, März 2007, S. 38ff.
- [79] Müller, Klaus-Rainer: Der Brückenschlag – Von Geschäftsprozessen zu (IT-) Ressourcen, BCI-Kongress zum Business Continuity Management, September 2006
- [80] Müller, Klaus-Rainer: Prozessorientierte Abnahmeorganisation, ix Magazin für professionelle Informationstechnik, 8/2002, S. 96ff.

- [81] Peine, Holger: Sicherheitsprüfwerkzeuge für Web-Anwendungen, Fraunhofer-Institut Experimentelles Software Engineering, Januar 2006
- [82] Alberts, Christopher, Dorofee, Audrey, Stevens, James, Woody, Carol: Introduction to the OCTAVE® Approach, Carnegie Mellon University, August 2003
- [83] Alberts, Christopher und Dorofee, Audrey: Managing Information Security Risks, Addison-Wesley, 2002
- [84] Swanson, Marianne: Security Self-Assessment Guide for Information Technology Systems, National Institute of Standards and Technology (NIST) Special Publication 800-26, November 2001
- [85] CERT/CC Statistics 1988 – 2004, CERT® Coordination Center®, www.cert.org/stats/cert_stats.html, 13.02.2005
- [86] Bundesamt für Sicherheit in der Informationsverarbeitung: BOSS (BSI OSS Security Suite), Einführung, <http://www.bsi.bund.de/produkte/boss/index.htm>, eingesehen am 13.08.2005
- [87] Carnegie Mellon University: Systems Security Engineering Capability Maturity Model, Model Description Document, Version 3.0, 15. Juni 2003
- [88] National Institute of Standards and Technology (NIST): Federal Information Technology Security Assessment Framework, 28. November 2000
- [89] Thiel, Christoph, Risiko Management – Einführung und Umsetzung, BITKOM-Forum IT-Sicherheit „Trends in der IT-Sicherheit“, 30.10.2002
- [90] <kes>/Microsoft-Sicherheitsstudie 2006, Lagebericht zur Informations-Sicherheit, Teil 2, <kes>, 5/2006, S. 40ff.
- [91] Jaeger, Stefan: Verbotene Protokolle, KES, 5/2000, S. 6ff.
- [92] Schuppenhauer, Rainer: GoDV-Handbuch, Beck Juristischer Verlag, 2006
- [93] Humphreys, Ted: State-of-the-art information security management systems with ISO/IEC 27001:2005, ISO insider, ISO Management Systems, January-February 2006
- [94] Zentraler Kreditausschuss: Financial Transaction Services (FinTS) – Security, Sicherheitsverfahren PIN/TAN inklusive Zwei-Schritt-TAN-Verfahren, Version 3.0, 9.2.2006
- [95] Bundesamt für Sicherheit in der Informationstechnik, Projektgruppe „Local Wireless Communication“: Sicherheit im Funk-LAN (WLAN, IEEE 802.11), 17.07.2002
- [96] Reinefeld, Alexander und Schintke, Florian: Concepts and Technologies for a WorldwideGrid Infrastructure, Zuse Institute Berlin (ZIB)
- [97] Sun Microsystems: Java™ Authentication and Authorization Service (JAAS), Reference Guide for the Java™ 2 SDK, Standard Edition, v 1.4

- [98] Sun Microsystems: Java™ Cryptographic Extension (JCE), Reference Guide for the Java™ 2 SDK, Standard Edition, v 1.4
- [99] Sun Microsystems: Java™ Secure Socket Extension (JSSE), Reference Guide for the Java™ 2 SDK, Standard Edition, v 1.4
- [100] American National Standards Institute (ANSI): Information Technology - Role Based Access Control, InterNational Committee for Information Technology Standards, ANSI/INCITS 359 - 2004
- [101] OASIS™: Universal Business Language (UBL), v2.0, 12. Dezember 2006
- [102] Harvard Research Group, Inc.: Highly available servers market assumptions 2000 – 2005, 2001

Glossar und Abkürzungsverzeichnis

A

Abwehrrechner (Bollwerk-Computer)

s. Bastion-Host

Access Control List (ACL)

s. Zugriffskontrollliste

Alarm – Alert

Ein Alarm ist ein optisches, akustisches oder sensorisches Signal, das die Zuständigen oder externe Hilfe leistende Stellen aufmerksam machen und zu Gegenmaßnahmen anhalten soll.

Anhängsel

s. Attachment

Anomalie – Anomaly

Bei Intrusion-Detection-Systemen werden unter Anomalien Abweichungen vom festgelegten Normalzustand verstanden.

Anomalieerkennung – Anomaly Detection

Die Anomalieerkennung wird von Intrusion-Detection-Systeme verwendet, um Abweichungen vom festgelegten Normalzustand zu erkennen.

ANSI

American National Standards Institute

Appliance

Eine Appliance (engl. für {Haushalts-}gerät) ist ein Computer, der als eine Art „Black Box“ schlüsselfertig bestimmte festgelegte Funktionalitäten in sich birgt.

Application Level Gateway (Anwendungsschicht-Gateway)

Das Application-Level- oder Anwendungsschicht-Gateway (s. a. [37], [66], [67], [70]) ist ein Firewall, der sich aus Sicht eines Client-Programms wie ein Server für den betreffenden Dienst darstellt.

Application Response Measurement (ARM)

Application Response Measurement (ARM) ist ein Standard der Open Group. Er definiert, wie Anwendungen Informationen zur Überwachung ihrer Verfügbarkeit, Performance und Kapazität bereit stellen können.

Attachment

Attachments sind Dateien, die als Anlage oder Anhängsel von E-Mails versandt werden.

Ausfallzeit – downtime

Als Ausfallzeit wird die Zeit bezeichnet, während der ein Prozess, eine Ressource, z. B. ein System oder eine Komponente, ein Produkt oder ein Service nicht im vereinbarten Umfang zur Verfügung steht.

Auslöser

Unter „Auslöser“ wird ein Ereignis verstanden, durch das der reguläre Geschäftsbetrieb beeinträchtigt wird. Je nach Schwere des Auslösers kann hieraus eine Störung, ein Notfall oder ein Katastrophenfall entstehen. Auslöser sind beispielsweise technische Defekte, wie Hardware-Ausfall, Naturereignisse wie Sturm, Flut, Tsunami, Erdbeben, kriminelle Handlungen, wie Sabotage, oder menschliches Versagen, wie Fehlbedienungen.

Authentifizierung – authentication

Durch Authentifizierung wird die Echtheit, z. B. der Identität oder einer Information, im Rahmen einer Prüfung bestätigt.

Authentisierung – authentication

Durch Authentisierung wird eine Information glaubwürdig bzw. rechtskräftig gemacht.

Autorisierung – authorization

Die Autorisierung stellt eine Bevollmächtigung oder Genehmigung dar.

B

Bastion-Host (Abwehrrechner, Bollwerk-Computer)

Firewalls in Computern, die sich zwischen dem zu sichernden und dem ungesicherten Netz befinden, sind Abwehrrechner, die als Bastion-Host (Bollwerk-Computer) bezeichnet werden.

Bedrohung – Threat

Eine Bedrohung ist die potenzielle Möglichkeit eines (unerwünschten) Schadens für Prozesse, Ressourcen (z. B. Anlagen, Systeme, Sachen und Menschen), Organisationen, Produkte und Leistungen.

Berechtigungskubus, Berechtigungswürfel

Der Berechtigungswürfel bzw. Berechtigungskubus veranschaulicht die Kombination aus Subjekt, Recht und Objekt. Er kann für jede der vier Sicherheitsschalen Zufahrts-, Zutritts-, Zugangs- und Zugriffsschutz genutzt werden.

Betriebseinflussanalyse – Operational Impact Analysis (OIA)

Mittels der Betriebseinflussanalyse (Operational Impact Analysis {OIA}) wird erhoben, welche Auswirkungen der Ausfall oder die

gravierende Beeinträchtigung eines Schutzobjektes, wie z. B. eines IT-Systems, eines Gebäudes oder eines Services, durch ein Ereignis hat.

Böswillige Software (Schadsoftware) – Malware

Böswillige Software umfasst z. B. Viren, Würmer und trojanische Pferde.

Botnet

Als Botnets werden Computernetze bezeichnet, die von Hackern bzw. Crackern kontrolliert werden. Sie bestehen aus Rechnern, die meist unbemerkt von ihren Besitzern durch Cracker übernommen wurden und ferngesteuert werden. Die Übernahme der Computer erfolgt über Schadprogramme, die z. B. als Anhang von E-Mails auf dem Computer eintrafen und geöffnet wurden, oder durch die Ausnutzung bekannter, aber nicht gepatchter Sicherheitslücken beim Besuch bössartiger Webseiten.

Die Anzahl übernommener Rechner nimmt zu. Sie werden von Crackern „vermietet“ und lassen sich von Ihnen oder den „Mietern“ dazu nutzen, Spam oder Phishing-Mails zu versenden, von Onlineshops unter Androhung von Distributed Denial of Service Attacken Schutzgeld zu erpressen, oder DDoS-Attacken zu fahren. Derartige Botnets können aufgrund ihres hohen Datenvolumens manches Servernetz in die Knie zwingen. Botnets lassen sich auch dazu verwenden, als Datei- oder Webserver illegale Software anzubieten, oder E-Mails mit neuen Schadprogrammen erstmalig und in großem Umfang zu verbreiten, bevor die Virensignaturen für Virens Scanner verfügbar sind.

Schützen kann man sich hiergegen z. B. durch zeitnahe automatische Virenupdates und zeitnahe Einspielung von Patches, die Nutzung eines Firewalls und das Nicht-Öffnen von E-Mail-Anhängen, die nicht klar zuordenbar sind. Auch sollten Links in E-Mails aus nicht sicherer Quelle nicht angeklickt werden.

Brandmeldeanlage (BMA) – fire alarm system

Brandmeldeanlagen gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Brände zu einem frühen Zeitpunkt zu erkennen und zu melden sowie direkte Hilferufe bei Brandgefahren abzusetzen.

Brute-Force-Attacke

Brute-Force-Attacken, also Angriffe, die auf „roher Gewalt“ beruhen, versuchen auf alle möglichen Arten, das Objekt der Attacke zu „knacken“. Brute-Force-Attacken zum Knacken von Passwörtern probieren beispielsweise alle möglichen Zeichenkombinationen (Buchstaben, Ziffern, Sonderzeichen) aus, bis das ge-

wünschte Passwort ermittelt ist. Bei Vorliegen eines einweg-verschlüsselten Passwortes kann durch rechenintensives Erzeugen und Verschlüsseln jedes potenziellen Passwortes nach dem gleichen Algorithmus so lange probiert werden, bis das verschlüsselte Ergebnis dem vorliegenden verschlüsselten Passwort entspricht. Aufgrund des Aufwands gelangen hierfür daher „social engineering“ und Wörterbuchattacken eher zum Einsatz.

BSI

1. British Standards Institution
2. Bundesamt für Sicherheit in der Informationstechnik

Bundesdatenschutzgesetz – Federal Data Protection Act

Das Bundesdatenschutzgesetz befasst sich mit dem Schutz personenbezogener Daten.

Business Impact Analysis (BIA)

Mittels der Business Impact Analysis (BIA) wird ermittelt, welche Auswirkungen der Ausfall oder die gravierende Beeinträchtigung eines Geschäftsprozesses durch Eintritt eines Ereignisses, z. B. eines Notfall oder einer Katastrophe, auf die Geschäftstätigkeit bzw. die Kerngeschäftsprozesse des Unternehmens hat. Im deutschen Sprachgebrauch findet sich hierfür der Begriff Geschäftseinflussanalyse oder Schutzbedarfsanalyse.

C

Certified Information Security Auditor™ (CISA™)

CISA™ ist eine Bezeichnung für Sicherheitsauditoren von Informationssystemen, die von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

Certified Information Security Manager™ (CISM™)

CISM™ ist eine Bezeichnung für Sicherheitsmanager von Informationssystemen, die von der Information Systems Audit and Control Association (ISACA®) zertifiziert wurden.

Challenge Handshake Authentication Protocol (CHAP)

Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentisierungsprotokoll, das in RFC 1994 definiert ist. Hierdurch können Benutzer von ihrem Client bei einer Authentisierungsinstanz (authenticator), z. B. einem Internet Service Provider (ISP), authentisiert werden. Voraussetzung ist, dass beide Kommunikationspartner das gleiche Geheimnis, z. B. ein Passwort, kennen und den gleichen Einweg-Hash-Algorithmus nutzen. Nach dem Verbindungsaufbau sendet der Server eine Zufallszahl (Challenge) an den Client. Der Client verkettet (konkati-

niert) seinen Identifier (Benutzerkennung) mit dem „Geheimnis“ (Passwort) und mit der Challenge (Zufallszahl). Hieraus berechnet er mittels des Einweg-Hash-Algorithmus einen Hashwert, den er als Antwort zurücksendet. Der Server prüft die Antwort mit der von ihm selbst errechneten. Bei Übereinstimmung war die Authentisierung erfolgreich. In zufälligen Zeitabständen sendet die Authentisierungsinstanz eine neue Challenge und wiederholt den Authentisierungsvorgang.

Challenge-Response-Verfahren

Das Challenge-Response-Verfahren dient der Authentifizierung mittels Einmal-Passwort. Der Host sendet an den PC des Benutzers eine Challenge. Der Benutzer erzeugt hieraus mittels eines Tokens eine Response und sendet sie an den Host zurück. Stimmt diese mit der erwarteten Response überein, ist die Authentifizierung erfolgreich.

Chief Compliance Officer (CCO)

Leiter jener Unternehmenseinheit, welche für die Konformität des Unternehmens verantwortlich ist, also für die Bekanntheit und Einhaltung gesetzlicher, aufsichtsbehördlicher und gegebenenfalls normativer Anforderungen.

Chipkarte – Smart Card

Eine Chipkarte hat die Größe einer Scheckkarte und enthält einen Chip mit einer CPU, I/O-Kanälen und einem nichtflüchtigen Speicher, auf den nur die CPU der Karte zugreifen können soll.

CIA

Akronym für Confidentiality, Integrity, Availability

CIA²

Akronym für Confidentiality, Integrity, Availability, Accountability

Circuit-Level-Gateway – Circuit Level Gateway

Ein Circuit-Level-Gateway (s. a. [37], [67]) ist ein Firewall, der auf Verbindungsebene filtert. Das Circuit-Level-Gateway arbeitet sozusagen als Vermittlungsstelle für das betreffende Protokoll.

Common Alerting Protocol (CAP)

Das Common Alerting Protocol (CAP) ist ein OASISTM-Standard, der ein allgemeines Format zum Austausch von Alarmen und öffentlichen Warnungen über alle Arten von Netzen beschreibt.

Compliance

s. Konformität

Computer Emergency Response Team (CERT[®])

Das Computer Emergency Response Team (CERT[®]) Coordina-

tion Center (CERT/CC) des Software Engineering Institute (SEI) an der Carnegie Mellon Universität wurde 1988 eingerichtet. Es ist ein Zentrum für Internet-Sicherheits-Expertise. Darüber hinaus haben Unternehmen ihre eigenen „CERTs“ etabliert, die präventiv und in kritischen Situationen kurzfristig auf Gefährdungen und Angriffe reagieren sollen. Für die Bundesverwaltung in Deutschland existiert seit 1. September 2001 das CERT-Bund. Europäische Behörden-CERTs haben sich in der European Government CERTs (EGC) Group informell zusammengeschlossen.

Computer Output on Laserdisk (COLD)

Computer Output on Laserdisk (COLD) bezeichnet die Übernahme von Computer-Output und dessen Archivierung auf digitalen optischen Speichermedien. COLD-Systeme speichern Computer-Output in einem elektronischen Format und stellen Funktionen zur Suche, Anzeige und Ausgabe zur Verfügung.

Computer Security Incident Response Team (CSIRT)

Das Computer Security Incident Response Team (CSIRT) ist eine Organisationseinheit eines Unternehmens, die reale oder vermutete sicherheitsrelevante Ereignisse behandelt. Sie nimmt die entsprechenden Meldungen entgegen, analysiert und bewertet sie und ergreift gegebenenfalls Maßnahmen zu deren Abwehr und gerichtlicher Verfolgung. Die Aufgaben schließen die forensische Analyse mit ein. Je nach unternehmensspezifischer Aufgabenzuordnung führt das CSIRT Schulungen und Sensibilisierungsmaßnahmen durch, beobachtet Trends und informiert die Zuständigen innerhalb des Unternehmens darüber. Das CSIRT ergreift präventiv Maßnahmen zur Weiterentwicklung der Sicherheitsstandards und Verbesserung des Sicherheitsniveaus. Das CSIRT kann ein dauerhaft eingerichtetes oder ad hoc zusammengerufenes Team sein.

Computervirus – computer virus

Ein Computervirus ist ein nicht selbständig ausführbarer Programmteil, der ein Wirtsprogramm benötigt sowie sich bei Aktivierung selbst vervielfältigen und Schaden verursachen kann, z. B. durch Löschen von Dateien. Ein Computervirus zeigt in diesen drei Punkten, nämlich der Notwendigkeit eines Wirts, der eigenständigen Verbreitung und der Schadensverursachung Parallelen zu biologischen Viren. Ein Computervirus besteht aus vier prinzipiellen Teilen: einer Viruskennung, dem Infektionsteil, dem Schadensteil und dem Sprungbefehl. Ist ein Programm infiziert, so ändert sich dessen Größe und Prüfsumme. Nach dem Start eines infizierten Programms und Aufruf des Computervirus

sucht der Infektionsteil nach anderen noch nicht infizierten Programmen und kopiert sich dort hinein. Anschließend führt er seine Schadfunktion aus und springt gegebenenfalls in den Programmcode zurück.

Content-Security-System – Content Security System

Content-Security-Systeme prüfen anhand eines unternehmensspezifisch festgelegten Regelwerks den Inhalt ein- und ausgehender E-Mails.

Cracker

Unter einem Cracker versteht man einen technisch sehr versierten Angreifer, dessen Angriffe darauf abzielen, sich einen Nutzen zu verschaffen und Dritten Schaden zuzufügen.

Cross-Site-Scripting (XSS)

Cross-Site-Scripting (XSS), manchmal auch abgekürzt mit CSS, dann aber verwechselbar mit Cascading Style Sheets, ist eine Angriffstechnik, bei der ein Angreifer Code, z. B. HTML, JavaScript® oder ActiveX, in eine Webseite einschleust. Der Angreifer veranlasst sein Opfer, eine bestimmte Webseite zu besuchen, indem er ihm beispielsweise einen entsprechenden Link in einer E-Mail zuschickt. Die ausgewählte Webseite ist für das Opfer vertrauenswürdig, z. B. die Webseite einer Bank. Gleichzeitig hat die Webseite aber eine Schwachstelle, die der Angreifer kennt: Sie nimmt Eingaben entgegen und gibt sie als Antwort auf bestimmte Anfragen ungeprüft als Ausgaben zurück. Der Angreifer fügt in die URL ausführbaren Code ein, der z. B. das Session-Cookie des Opfers an den Rechner des Angreifers schickt. Der Angreifer kann nun ein „Session-Hijacking“ („Sitzungsentführung“) durchführen, also unter der Identität des Opfers mit der kompromitierten Webseite arbeiten. Ähnliche Angriffsszenarien ergeben sich u. a. bei Foren und Gästebüchern, wenn die eingegebenen Daten ungeprüft gespeichert und bei neuen Anfragen an den Anfragenden ausgegeben werden.

D

Demilitarisierte Zone

s. entmilitarisierte Zone

Digitales Rechtemanagement (DRM) – Digital Rights Management (DRM)

Digitales Rechtemanagement (DRM) bzw. Digital Rights Management bezeichnet ein Verfahren, durch das sich Rechte an elektronisch vorliegendem geistigem Eigentum mittels Kryptogra-

phie schützen lassen sowie deren Nutzung abrechnen lässt. Schutzobjekte sind z. B. digital vorliegende Ton- und Filmaufnahmen sowie elektronische Dokumente und Bücher, aber auch Software-Produkte eines Unternehmens. Ziel ist es, die Einhaltung der Nutzungsrechte mit technischen Mitteln zu erzwingen.

Ein DRM besteht prinzipiell aus drei Komponenten: dem Content Server, dem License Server und dem Client. Der Content Server verschlüsselt die zu schützenden Daten (Content) so, dass sie sich nur mit dem Schlüssel der dazugehörigen Lizenz entschlüsseln lassen. Der Nutzer lädt das verschlüsselte Paket (Content) auf seinen Client herunter. Ruft der Nutzer das verschlüsselte Paket auf, so schickt der Client eine Anfrage mit der Identität des Nutzers und des Contents an den License Server. Dieser identifiziert den Nutzer. Ist der Nutzer – gegebenenfalls nach Bezahlung – zur Nutzung des Contents berechtigt, erstellt und übermittelt der License Server die Lizenz an den Client. Hiermit entschlüsselt der Client den Content, so dass der Nutzer ihn verwenden kann.

Digitales Wasserzeichen – Digital Watermarking

Digitale Wasserzeichen sind zusätzliche Informationen, die mittels Steganographie in digitale Dateien eingebracht werden, um Urheberfragen klären und damit Urheberrechte schützen zu können.

Direct Attached Storage (DAS)

Direct Attached Storage (DAS) bezeichnet eine Speichereinheit, die mit dem Computer direkt verbunden ist.

Discretionary Access Control (DAC)

Die Discretionary Access Control (DAC, diskrete Zugriffskontrolle) ermöglicht einem Datei-Eigentümer die Festlegung, welche Nutzer welchen Zugriff auf seine Datei haben.

Dokumentenlebenszyklusmanagement (DLM) – Document Lifecycle Management (DLM)

Dokumentenlebenszyklusmanagement bezeichnet die Steuerung, Verfolgung und Verwaltung von Dokumenten während ihres Lebenszyklus von der Erstellung über die Aufnahme, Speicherung, Archivierung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung.

Domain Name Services (DNS)

Domain Name Services (DNS) übersetzen alphanumerische Internetadressen (URL) in eine IP-Adressen. DNS-Server sind also das „Telefonbuch“ des Internet und damit dessen Rückgrat.

DoS-Angriff – Denial of Service (DoS) Attack

Angriff, bei dem ein Zielsystem oder –Netzwerk lahm gelegt wird.

Dynamic Host Configuration Protocol DHCP

Das Dynamic Host Configuration Protocol (DHCP) ist in der Version für IPv6 (DHCPv6) in RFC 3315 spezifiziert und für IPv4 in RFC 2131. Ein DHCP-Server kann einem Computer im Netz dynamisch und zeitlich begrenzt eine wiederverwendbare IPv6-Adresse zuweisen. Die DHCP-Nachrichten werden mittels UDP ausgetauscht.

E**ebXML**

electronic business eXensible Markup Language (ebXML)

EICAR

Das European Institute for Computer Antivirus Research (EICAR) zielt darauf ab, die Bemühungen gegen das Schreiben und die Verbreitung böswilligen Codes, gegen Computerkriminalität und –missbrauch sowie die böswillige Nutzung persönlicher Daten zusammenzuführen.

Einbruchmeldeanlage (EMA) - burglar alarm system

Einbruchmeldeanlagen gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Flächen und Räume auf unbefugtes Eindringen sowie Gegenstände auf unbefugte Wegnahme zu überwachen.

Eintrittswahrscheinlichkeit - probability of occurrence

Die Wahrscheinlichkeit, mit der ein Ereignis eintritt, heißt Eintrittswahrscheinlichkeit. Sie wird bei der Bewertung des als Schadensausmaß $\times$ Eintrittswahrscheinlichkeit definierten Bruttoisikos bzw. der Kosten-Nutzen-Abwägung zur Festlegung des Umfangs von Sicherheits- und Kontinuitätsmaßnahmen genutzt. Hierbei muss beachtet werden, dass Eintrittswahrscheinlichkeiten oftmals retrospektiv (ex post) ermittelt werden. D. h. die Eintrittswahrscheinlichkeit wird anhand der zurückliegenden Ereignisse innerhalb eines vorgegebenen Zeitraums ermittelt. Generell ist bei Wahrscheinlichkeiten daran zu denken, dass ein Ereignis, das z. B. alle 100 Jahre auftritt, auch morgen, heute, oder jetzt auftreten kann.

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) bezeichnet den elektronischen Dokumentenaustausch mit formatierten Strukturen, die von IT-Systemen weiterverarbeitet werden können.

Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)

Electronic Data Interchange for Administration Commerce and

Transport (EDIFACT) ist eine internationale Normenreihe (DIN ISO 9735) zur Standardisierung von Nachrichteninhalten.

Elektronische Falschmeldung/„Ente“ – Hoax

E-Mail, die vor einem neuen Virus warnt, jedoch eine Falschmeldung („Ente“) ist. Insbesondere ungeschulte Computernutzer sollen hierdurch zu schädlichen Aktionen veranlasst werden, z. B. Weiterleiten der E-Mail und Löschen von angeblich verseuchten Dateien. Aktuelle Informationen hierzu finden sich beispielsweise unter www.bsi.bund.de/av/hoaxes/hoaxes.htm.

EMA

s. Einbruchmeldeanlage

Entmilitarisierte Zone – Demilitarized Zone (DMZ)

Eine entmilitarisierte Zone ist der Bereich zwischen einem äußeren und einem inneren Firewall. In dieser Zone werden z. B. Web-Server angesiedelt.

Exploit

Exploits sind Programme, die Sicherheitslücken oder Fehlfunktionen von Computerprogrammen nutzen, um in diese einzudringen. Sie werden von Hackern bzw. Crackern geschrieben und auch als Hack-Werkzeuge bezeichnet.

F

Falsch negativ – False negative

Ist das Ergebnis einer Prüfung, z. B. zur Zutritts- oder Zugangskontrolle, falsch negativ, so erfolgt fälschlicherweise eine Ablehnung.

Falsch positiv – False positive

Ist das Ergebnis einer Prüfung, z. B. zur Zutritts- oder Zugangskontrolle, falsch positiv, so erfolgt fälschlicherweise eine Freigabe.

False Acceptance Rate (FAR)

Die False Acceptance Rate (FAR) bzw. Falsch-Akzeptanzrate gibt an, wie oft statistisch ein Objekt fälschlicherweise akzeptiert wird. Beim Einsatz biometrischer Verfahren, beispielsweise zur Zutritts- oder Zugangskontrolle, ist diese Angabe extrem sicherheitsrelevant, da eine fälschliche Erkennung unberechtigten Personen Zutritt oder Zugang ermöglicht.

False Rejection Rate (FRR)

Die False Rejection Rate (FRR) bzw. Falsch-Rückweisungsrate

gibt an, wie oft statistisch ein Objekt fälschlicherweise abgelehnt wird. Beim Einsatz biometrischer Verfahren, beispielsweise zur Zutritts- oder Zugangskontrolle, bedeutet dies, dass berechnete Personen fälschlicherweise abgewiesen werden. Dies mindert potenziell die Akzeptanz eines solchen Systems und kann zu kritischen Situationen führen.

Fibre Channel (FC)

Fibre Channel umfasst einen Satz von Standards für eine Technologie, die Hochgeschwindigkeitsdatenübertragung zwischen Computern ermöglicht. FC unterstützt Punkt-zu-Punkt-, Switch- und Loop-Technologien.

Financial Transaction Services (FinTS)

Die Financial Transaction Services (FinTS) sind ein Standard des Zentralen Kreditausschusses (ZKA). Er dient der Vereinheitlichung der Schnittstelle zwischen Bankkunde und Finanzinstitut. Die Version 4.0 der FinTS liegt seit 2004 vor. Sie besteht aus FinTS Formals, FinTS Messages und FinTS Security. FinTS Formals enthält allgemeine Festlegungen zur Syntax, zum Nachrichtenaufbau und zum Dialogablauf. FinTS Messages spezifiziert Geschäftsvorfälle und Belegungsrichtlinien für Finanzdatenformate, wie DTAUS, DTAZV und S.W.I.F.T..

FinTS Security beschreibt das PIN/TAN- (FinTS PIN/TAN) und das HBCI-Legitimationsverfahren (FinTS HBCI). FinTS HBCI ermöglicht wie das HBCI die elektronische Signatur, z.B. per Chipkarte. Seit der Version 3.0 unterstützt FinTS HBCI die Bankensignaturkarte, mit der rechtsverbindliche Unterschriften im Onlinebanking möglich sind. Das FinTS HBCI realisiert ein hohes Sicherheitsniveau, FinTS PIN/TAN eine hohe Mobilität. [94]. FinTS V4.0 verwendet XML-Technologien, wie XML-Scheme, -Signature und -Encryption, und unterstützt Web-Services wie WSDL und SOAP.

Fingerabdrucknehmen – Fingerprinting

Der IP-Stack jedes Rechners hat Eigenheiten, die sich insbesondere in der Antwort des Betriebssystems auf fehlerhafte Pakete bemerkbar machen. Es hinterlässt sozusagen einen Fingerabdruck. Um über das Netz an Informationen über das Betriebssystem zu gelangen, dient das „Fingerabdrucknehmen“. Beim aktiven Fingerabdrucknehmen werden fehlgeformte Pakete an das Zielsystem gesendet und die Antwort mit einer Datenbank verglichen, in der die Reaktionen verschiedener Betriebssysteme auf fehlgeformte Pakete zuvor eingetragen wurden. Beim passiven Fingerabdrucknehmen werden die Spuren des sendenden Betriebssys-

tems in den ankommenden Paketen analysiert. Charakteristika sind beispielsweise die „time to live“ (TTL) ausgehender Pakete, die „window size“, das „don't fragment bit“ (DF) und die Festlegung des „type of service“ (TOS).

Firewall

Ein Firewall („Brandschutzmauer“) ist eine Netzkomponente, die zwei Netze mit unterschiedlichem Sicherheitsniveau so miteinander verbinden soll, dass das zu schützende Netz vor Übergriffen aus dem anderen Netz geschützt wird.

Forensische Informatik

Die forensische Informatik beschäftigt sich mit der Spurensuche auf Computern nach erfolgreichen Angriffen.

Forum of Incident Response and Security Teams (FIRST)

Das globale Forum of Incident Response and Security Teams (FIRST) bringt eine Vielzahl von Computer Security Incident Response Teams aus öffentlichen und kommerziellen sowie Bildungsbereichen zusammen. Ziel ist die Förderung der Zusammenarbeit und Koordination im Hinblick auf die Vorbeugung gegenüber sicherheitsrelevanten Ereignissen, die schnelle Reaktion darauf sowie der Informationsaustausch.

Funk-LAN – Wireless Local Area Network (WLAN)

Funk-LANs (WLAN) stellen ein drahtloses lokales Netz dar. Sie basieren auf dem vom Institute of Electrical and Electronics Engineers (IEEE) 1997 festgelegten Standard IEEE 802.11. Da sie einfach zu installieren sind, kommen sie bei temporären Installationen zum Einsatz, z. B. auf Messen, aber auch bei langfristigerer Nutzung, z. B. auf Flughäfen und Bahnhöfen. Der Netzzugang erfolgt über Hot Spots. 1999 wurde die Erweiterung IEEE 802.11b verabschiedet. Die Kompatibilität von Produkten zu IEEE 802.11 dokumentiert die Herstellervereinigung Wireless Ethernet Compatibility Alliance (WECA) durch Vergabe des Wi-Fi®-Zertifikats. Funk-LANs gemäß IEEE-Standard 802.11 wiesen Schwachstellen auf [95]. Um die Schwachstellen des Standards IEEE 802.11 zu beseitigen, setzte IEEE eine Arbeitsgruppe zur Entwicklung des Standards 802.11i ein, der Mitte 2004 verabschiedet wurde. Die in IEEE 802.11i beschriebene Sicherheitsarchitektur nutzt zur Authentisierung das Extensible Authentication Protocol (EAP) und zur Verschlüsselung AES.

Für 2007 ist der Standard IEEE 802.11n angekündigt, der zu 802.11b und 802.11g abwärtskompatibel sein soll. Gegenüber 802.11g soll 802.11n über eine größere Reichweite und eine höhere Übertragungsrate verfügen.

Funktionsstrennung – Segregation of Duties

Funktionsstrennung beschreibt das Prinzip, Funktionen, die nicht miteinander vereinbar sind, zu trennen, d. h. ein und dieselbe Person darf nicht beide Funktionen ausführen. Beispielsweise dürfen Personen einer genehmigenden oder einer prüfenden Funktion, wie z. B. die Revision, die Qualitätssicherung oder ein Testteam, nicht gleichzeitig auch der geprüften Funktion angehören.

G**Gefahrenmeldeanlage (GMA)**

Gefahrenmeldeanlagen dienen dazu, Gefahren für Personen und Sachen zu erkennen und zu melden.

Geschäftseinflussanalyse – Business Impact Analysis (BIA)

s. Schutzbedarfsanalyse

Geschäftskritische Unterlagen – vital records

„Lebenswichtige“, d. h. geschäftskritische Unterlagen und Zeichnungen (vital records) sind für den Geschäftsbetrieb unverzichtbar und müssen daher – auch im Notfall – verfügbar sein und erhalten bleiben. Beispiele hierfür können geheime Produktionsverfahren und –formeln, Fahrzeugbriefe, Informationen über und Verträge mit Kunden, Lieferanten, Dienstleistern, Versicherungen und Mitarbeitern, Vollmachtenregelungen, etc. sein.

Grids

Grids sind weltweit vernetzte Computer unterschiedlicher Organisationen bzw. Unternehmen. Die Computer stellen dabei die „Knotenpunkte“ des „Gitters“ dar. Das Zuse Institut Berlin [96] unterscheidet drei Arten von Grids: „Resource Grids“, „Information Grids“ und „Service Grids“. Resource Grids dienen der weltweiten organisations- bzw. unternehmensübergreifenden Nutzung von Ressourcen, wie Rechnern, Speichern und Datenarchiven. Hierbei sind Sicherheits-, Kontinuitäts- und Abrechnungsaspekte zu berücksichtigen. Information Grids stellen jederzeit an jedem Ort der Welt zu beliebigen Themen einem anonymen Nutzer kostenlos Informationen bereit, oftmals nur in HTML, zunehmend in XML. Ein Beispiel für ein Information Grid ist das Internet. Service Grids schließlich stellen Services bereit, beispielsweise in Form von Identifikations- und Authentifizierungsdiensten und Suchmaschinen.

H

Hacker

Unter einem Hacker versteht man einen technisch sehr versierten Angreifer, dessen Angriffe darauf abzielen, Schwachstellen in ITK-Systemen aufzudecken. Primäres Ziel ist es dabei üblicherweise jedoch nicht, sich persönlich wirtschaftliche Vorteile zu verschaffen und Dritten einen direkten wirtschaftlichen Schaden zuzufügen, sondern auf Schwachstellen hinzuweisen.

Solange dies unter Nutzung eigener oder hierfür zur Verfügung gestellter Systeme und vertrauliche Bekanntgabe der Schwächen nur an die jeweiligen Hersteller oder Auftraggeber erfolgt, mag dies nachvollziehbar sein.

In der fachfremden Öffentlichkeit ist die Unterscheidung zwischen Hacker und Cracker eher wenig zu beobachten. Ursache mag sein, dass das Eindringen in Systeme Dritter – sei es mit oder ohne Selbstbereicherungs- oder Schädigungsabsicht – dennoch Schaden an Systemen, zusätzlichen Aufwand und Imageschäden nach sich ziehen kann. Auch das Schreiben und Verfügbarmachen von Exploits zur Demonstration der Sicherheitslücken stellt eine potenzielle Gefahr für Dritte dar.

Basierend auf einer Idee in Bruce Schneiers Buch „Secrets & Lies“ mag das folgende leicht abgewandelte Beispiel dies vom Prinzip her veranschaulichen: Wie würde es jemand empfinden, wenn ein Dritter versuchen würde, in dessen Privathaus oder Unternehmen einzudringen, ihm dies auch unbemerkt gelänge, er keinerlei Schaden anrichten und nichts verändern würde und er dies im Interesse der Allgemeinheit ohne dessen Zustimmung publizieren würde, damit dieser sein Privathaus oder Unternehmen besser absichert?

Harvester

Harvester (Erntemaschinen) sind eine Spezialform der Webcrawler. Sie durchsuchen das World Wide Web nach E-Mail-Adressen und „ernten“ diese. Die E-Mail-Adressen werden anschließend z. B. für Werbe-E-Mails (Spam) genutzt.

Hazard and Operability Analysis (HAZOP)

Die Hazard and Operability Analysis (HAZOP), d. h. die Gefahren- und Betriebsfähigkeitsanalyse, ist eine formale Methode, um das Verhalten von Systemen bei unterschiedlichen Fehlern zu ermitteln sowie Maßnahmen zu deren Absicherung zu ergreifen. HAZOP wurde ursprünglich in der chemischen Industrie eingesetzt und später zur Anwendung auf Software erweitert.

Home Banking Computer Interface (HBCI)

Das Home Banking Computer Interface (HBCI) wurde 1996 vom Zentralen Kreditausschuss (ZKA) als Standard für das Online-banking geschaffen. Ziel war und ist die Vereinheitlichung der Schnittstelle zwischen Bankkunden und Finanzinstituten. Die Weiterentwicklung des HBCI hat ihren Niederschlag in den Financial Transaction Services (FinTS) des ZKA gefunden.

I**Informationslebenszyklusmanagement (ILM) – Information Life-cycle Management (ILM)**

Informationslebenszyklusmanagement bezeichnet die Kosten-Nutzen-optimierte Steuerung, Verfolgung, Speicherung und Verwaltung von Informationen jeglicher Art und jeglichen Typs während ihres Lebenszyklus von der Erstellung über die Aufnahme, Speicherung, Archivierung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung. Ziel ist es, Informationen entsprechend ihrer geschäftlichen Bedeutung und ihren Sicherheitsanforderungen sowie ihrer Zugriffs- und Änderungshäufigkeit zu minimalen Kosten rechtzeitig am richtigen Ort verfügbar zu haben. Dies erfordert eine kontinuierliche Optimierung der Architektur aus Prozessen und Verfahren sowie Ressourcen und Technologien.

Ingenieurmäßige Sicherheit – safety and security engineering

Unter ingenieurmäßiger Sicherheit versteht der Autor die Erhebung, Pflege und jederzeitige Erfüllung der Sicherheits- und Kontinuitätsanforderungen eines Unternehmens durch den systematischen Aufbau und Betrieb sowie die systematische Pflege und Weiterentwicklung der Sicherheit und Kontinuität auf der Basis anerkannter Prinzipien, Methoden, Hilfsmittel und Werkzeuge. Ingenieurmäßige Sicherheit führt somit zur Festlegung prozessualer und methodischer, ressourcenspezifischer, technologischer und personeller sowie organisatorischer Elemente zur effizienten und zielgerichteten Erfüllung von Sicherheits- und Kontinuitätsanforderungen.

Institut der Wirtschaftsprüfer (IDW)

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) ist ein eingetragener Verein, der Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften Deutschlands auf freiwilliger Basis vereint.

International Engineering Consortium (IEC)

Das International Engineering Consortium (IEC) ist eine Non-

Profit-Organisation mit dem Ziel, den weltweiten technologischen und wirtschaftlichen Fortschritt im Bereich hochtechnisierter Industrien und universitärer Gemeinschaften zu katalysieren.

International Organization for Standardization (ISO)

Die International Organization for Standardization (ISO) ist ein Netz nationaler Standardisierungsinstitute. In ihr sind 148 Länder vertreten, jedes durch ein Mitglied. Das Zentralsekretariat der ISO hat seinen Sitz in Genf in der Schweiz und koordiniert das Gesamtsystem.

Die ISO ist keine staatliche Organisation. Ihre Mitglieder sind daher keine Delegationen nationaler Regierungen.

Manch einer mag sich schon gefragt haben, warum die Abkürzung ISO heißt, wo die englischen Anfangsbuchstaben doch „IOS“ und die französischen „OIN“ (Organisation Internationale de Normalisation) ergäben. Dies rührt daher, dass zu Beginn entschieden wurde, das Wort aus dem griechischen „isos“ (ισος: gleich) abzuleiten.

Die ISO verwendet folgende Abkürzungen für den Status Ihrer Normen:

- AWI= Approved Work Item
- CD= Committee Draft
- DIS= Draft International Standard
- FDIS= Final Draft International Standard
- ISO/TR= ISO Technical Report
- NP= New Work Item Proposal
- PRF= Proof of a new International Standard
- WD= Working Draft

Internet Engineering Task Force (IETF)

Die Internet Engineering Task Force (IETF) ist eine offene internationale Gemeinschaft, die sich mit der Weiterentwicklung der Internet-Architektur und dem reibungslosen Betrieb des Internet beschäftigt.

Internet Message Access Protocol (IMAP)

Das Internet Message Access Protocol (IMAP), Version 4, beschrieben in RFC 3501, erlaubt es einem Computer (Client), auf E-Mails zuzugreifen, die sich auf einem Server befinden sowie diese zu verändern und zu verwalten. Im Gegensatz zu POP ermöglicht IMAP den Zugriff von Clients an verschiedenen Standorten, z. B. von zu Hause, vom Büro oder von unterwegs. Die zentrale Speicherung und Archivierung der E-Mails sowie die von IMAP auf dem Server bereitgestellten Funktionen, z. B. zum Suchen, sind auch für leistungsschwächere Clients nützlich. Bei Einsatz von TCP nutzt IMAP standardmäßig den Port 143.

IMAP ist wie POP ein Klartextprotokoll. Es gibt jedoch Varianten, die z. B. eine verschlüsselte Übertragung über TLS nutzen. Diese Variante heißt IMAPs und nutzt standardmäßig den TCP-Port 993.

Intrusionserkennungssystem – Intrusion Detection System (IDS)

Intrusion-Detection-Systeme dienen dazu, Angriffe frühzeitig zu erkennen, indem der Datenverkehr auf dem Netz analysiert wird.

IP-Identitätsvorspiegelung – IP-Spoofing

Vortäuschung einer IP-Identität

IP-Maskerade – IP-Masquerading

IP-Maskerade bezeichnet die Maskierung/das Verbergen (interner) IP-Adressen durch Übersetzung in andere (externe) IP-Adressen. Hierdurch lassen sich interne IP-Adressen, über die gegebenenfalls Rückschlüsse auf das interne Netz möglich wären, nach außen verbergen.

IPsec

Das IP Security Protocol (IPsec) dient der Sicherung des IP-Verkehrs über das Internet durch Bereitstellung kryptographischer Dienste.

ISiPyr – ISiPyr (Information Safety/Security Pyramid)

IT- bzw. ITK-Sicherheitspyramide

IT-Compliance

s. Konformität

IT-Governance

Unter IT- bzw. ITK-Governance ist die an der Geschäftstätigkeit, der Unternehmensstrategie und den Unternehmenszielen ausgerichtete gute und verantwortliche Leitung der IT bzw. ITK zu verstehen. Sie sollte sich u. a. orientieren an relevanten gesetzlichen, aufsichtsbehördlichen und vergleichbaren Vorgaben und Standards zur Leitung, Steuerung und Überwachung der IT bzw. ITK, an diesbezüglichen international und national anerkannten Normen und Standards, an Good und Best Practices und De-facto-Standards sowie an vertraglichen Vereinbarungen (s. a IT-Compliance). Dies beinhaltet den wirtschaftlichen Einsatz von Ressourcen, das Risikomanagement mit der Optimierung und zielgerichteten Steuerung von Risiken und die angemessene Berücksichtigung aller Bezugsgruppen.

Eine ähnliche, aber weniger detaillierte Definition wählt das IT Governance Institute® in COBIT® 4.0, indem es – frei übersetzt – IT-Governance als Verantwortlichkeit der Führungskräfte und -gremien bezeichnet, durch Führung, Organisationsstruktur und Prozesse dafür zu sorgen, dass die IT die Strategien und Ziele des

Unternehmens bzw. der Organisation trägt und ausweitet.

ITK – ICT (information and communication technology)
Informations- und Kommunikationstechnologie

ITKSiPyr – ICTSaSePyr
ITK-Sicherheitspyramide

ITSCM
IT Service Continuity Management

ITU-T

Die International Telecommunications Union (ITU) ist eine internationale Organisation, in der Regierungen und die Privatwirtschaft zusammenarbeiten, um den Betrieb von Telekommunikationsnetzen und –services zu koordinieren, Standards zu erstellen sowie die Kommunikationstechnologie weiterzuentwickeln. ITU spielt eine wesentliche Rolle bei der Verwaltung und Steuerung des Funkfrequenzspektrums. Dies stellt sicher, dass funkbasierte Systeme, wie beispielsweise Mobilfunkgeräte, Navigationsgeräte für Flugzeuge und Schiffe, Satellitenkommunikationssysteme, Rundfunk und Fernsehen reibungslos arbeiten und ihre Dienste zuverlässig bereitstellen können.

Der Telecommunication Standardization Sector (ITU-T) entwickelt internationale technische Standards und Betriebsstandards – im ITU-Sprachgebrauch sogenannte Empfehlungen (Recommendations) – sowie Abrechnungsprinzipien. Ziel der ITU-T ist es, die nahtlose Verbindung weltweiter Kommunikationsnetze und –systeme zu fördern.

Internationale Standards der Informations- und Telekommunikationstechnologie (ITK) gewinnen zunehmend an Bedeutung, einerseits wegen der Globalisierung und andererseits, weil die Telekommunikation ein Eckpfeiler der heutigen Wirtschaft ist. Der Austausch von Sprach-, Daten- und Videonachrichten erfordert Standards für Sender und Empfänger, wie z. B. ADSL, GSM, JPEG, MPEG und TCP/IP.

Das Netz der nächsten Generation (next-generation network {NGN}) ist ein entscheidendes Forschungsgebiet der ITU-T, da Netzbetreiber überall auf der Welt IP-basierte Infrastrukturen migrieren möchten. Diese Konvergenz von u. a. Internet Protokollen (IP), öffentlichen Netzen, Kabelfernsehen (CATV), Wireless LANs und Mobilfunktechnologie erfordert internationale Standards.

J**Java™ Authentication and Authorization Service (JAAS)**

Der JAVA™ Authentication and Authorization Service (JAAS) ist ein Paket, das Dienste zur Authentisierung und Zugriffskontrolle von Nutzern ermöglicht. JAAS ist in Java 2 SDK, v. 1.4, integriert. [97]

Java™ Cryptographic Extension (JCE)

Die JAVA™ Cryptographic Extension (JCE) stellt ein Rahmenwerk und Implementierungen zur Verfügung zur Verschlüsselung und zur Schlüsselerzeugung sowie Message Authentication Code (MAC) Algorithmen. JCE ist in Java 2 SDK, v. 1.4, integriert und unterstützt symmetrische und asymmetrische Verschlüsselung. Das JCE API bietet Verschlüsselung an u. a. für DES, IDEA, Triple DES, Blowfish und RSA. [98]

Java™ Secure Socket Extension (JSSE)

Die Java™ Secure Socket Extension (JSSE) ermöglicht eine gesicherte Kommunikation über das Internet. JSSE stellt hierfür sowohl ein Application Programming Interface (API) Rahmenwerk bereit als auch dessen Implementierung. Sie enthält eine Java™-Version der SSL (Secure Sockets Layer) und TLS (Transport Layer Security) Protokolle. JSSE beinhaltet Funktionalitäten für die Datenverschlüsselung, Serverauthentisierung, Nachrichtenintegrität und optional Clientauthentisierung. [99]

K**Kerberos™ – Kerberos™**

Kerberos™ ist ein ticket-basiertes Authentisierungsverfahren, das vom MIT entwickelt wurde. Es ist benannt nach dem Höllenhund Kerberos, dem Sohn des Typhon und der Echidna, der in der griechischen Mythologie den Eingang zum Hades, der Unterwelt, benannt nach dem Gott Hades, bewachte. Er ließ keinen der Eingetretenen mehr heraus. Nur Orpheus und Herakles zwangen ihn. Wenngleich es sich also um eine Bewachung des Ausgangs aus dem Hades, der Unterwelt, handelt, liegt das „tertium comparationis“, d. h. die Parallele zum Kerberos™ des MIT, offensichtlich darin, dass hierdurch auch gleichzeitig der Eingang zur Welt außerhalb des Hades „bewacht“ ist, so wie Kerberos™ den Zugang zu Systemen überwacht. Dass der Höllenhund in oben genannten Ausnahmefällen besiegt wurde, könnte als unerwünschte Parallele zu sehen sein.

Key-Logger

Key-Logger protokollieren die Tastatureingaben des Nutzers. Es existieren sowohl Software- als auch Hardware-Key-Logger. Software-Key-Logger kommen einerseits als ordnungsgemäße Software-Programme zum Einsatz, werden andererseits aber auch von Angreifern über Trojaner verbreitet.

Hardware-Keylogger lassen sich zwischen Tastatur und Rechner stecken, entweder am PS/2-Port oder an der USB-Schnittstelle. Sie können derzeit bis zu 2 Mio. Tastatureingaben aufzeichnen. Im Gegensatz zu Software-Key-Loggern verbleiben nach der Entfernung der Komponente keine verräterischen Datenspuren auf dem überwachten Computer.

Zum Schutz vor einem Mitschnitt der Tastatureingabe erfolgt verschiedentlich der Übergang zu mausbasierten Eingaben, bei denen virtuelle Tastaturen, z. B. ein Ziffernblock, am Bildschirm angezeigt werden, deren Felder zur Eingabe mit der Maus angeklickt werden.

Kommunales Netz – Metropolitan Area Network (MAN)

Ein MAN dient der Zusammenschaltung von Systemen und Netzen in Ballungsräumen.

Konformität – Compliance

Konformität (Compliance, d. h. Übereinstimmung, Einhaltung) bezeichnet die Kenntnis und Einhaltung gesetzlicher, aufsichtsbehördlicher und vergleichbarer sowie vertraglicher und normativer Vorgaben und Anforderungen, d. h. die Gesetzeskonformität und die Einhaltung von Standards, Bestimmungen und Verträgen. Dies sicherzustellen ist Aufgabe des Konformitäts- bzw. Compliance Managements.

Vorgaben ergeben sich hierbei insbesondere aus Gesetzen und darauf aufbauenden Ausführungsbestimmungen sowie dementsprechenden Prüfungsbestimmungen der Wirtschaftsprüfer. Ebenfalls zu beachten sind hierbei Normen und De-facto-Standards sowie Good und Best Practices.

Unterthemen der Konformität bzw. Compliance sind die IT- bzw. ITK-Compliance. Sie konzentriert sich auf die Kenntnis und Einhaltung der Anforderungen an die IT bzw. ITK, die z. B. von Gesetzen oder Standards vorgegeben oder aus ihnen abgeleitet sind. Derartige Anforderungen ergeben sich in Deutschland u. a. aus dem HGB und den GoBS, aus Datenschutzgesetzen, wie dem BDSG, und dem Urheberrechtsgesetz. Für Banken formulieren das KWG und die MaRisk Vorgaben. Weitere Anforderungen sind in internationalen und nationalen Normen, Standards und Good bzw. Best Practices enthalten, wie z. B. der ISO 13335, der ISO 17799 und der ISO 27001, in COBIT® und in den Best Practi-

ces à la ITIL® sowie dem IT-Grundschutzhandbuch des BSI mit seinen umfangreichen Grundschutzkatalogen. Nicht zu vergessen sind die Prüfungsstandards der Wirtschaftsprüfer, z. B. FAIT 1, FAIT 2 und FAIT 3.

Die Sicherheitsmanagementpyramide nach Dr.-Ing. Müller stellt ein integratives und ganzheitliches Vorgehensmodell zur systematischen Umsetzung dieser Anforderungen dar.

Kontinuitätsmanagement – Business Continuity Management (BCM)

Das Kontinuitätsmanagement bzw. das Management der Geschäftskontinuität bzw. das Business Continuity Management (BCM) beschreibt das Vorgehen zur Sicherstellung der geordneten, vereinheitlichten und effizienten sowie jederzeitigen ausreichenden Handlungsfähigkeit des Unternehmens auch in Not- und Katastrophenfällen, die das Überleben des Unternehmens sichert. Dies beinhaltet die Verpflichtung der Unternehmensleitung, die Prozess- und Strukturorganisation, das Vorgehensmodell samt Rahmenwerk, z. B. anhand der BCM-Pyramide nach Dr.-Ing. Müller, die Erhebung der externen und internen Anforderungen sowie potenzieller Bedrohungen und deren Eintrittswahrscheinlichkeit, die Ermittlung des Schadenspotenzials für den Fall, dass die Bedrohungen eintreten, die angemessene Absicherung vor diesen Bedrohungen, das Testen, Monitoring, Controlling und Reporting sowie die kontinuierliche bzw. regelmäßige Pflege, Prüfung und Weiterentwicklung einschließlich Schulung, Sensibilisierung und Übung. Die Integration des BCM in die Lebenszyklen sowie in die Prozesse, Ressourcen, Dienstleistungen und Produkte ist ein weiterer wesentlicher Bestandteil des BCM. Deren Umsetzung führt – wie es der Autor nennt – zu lebenszyklus-, prozess-, ressourcen-, dienstleistungs- und produktimmanenter Kontinuität.

Wie bereits an anderer Stelle erläutert ist BCM ein integraler Teil der dreidimensionalen Sicherheitspyramide nach Dr.-Ing. Müller. Dies liegt darin begründet, dass Geschäftskontinuität mehr umfasst als nur den Schutz von Ausfällen der Prozesse, Ressourcen, Produkte oder Dienstleistungen, nämlich auch den Schutz vor Angriffen, kriminellen Handlungen, menschlichem Versagen, Fehlverhalten, etc. Alle diese Bedrohungen können auf unterschiedliche Art zu einer Einschränkung oder gravierenden Störung des regulären Geschäftsbetriebs bis hin zur Handlungsunfähigkeit des Unternehmens führen.

Damit entspräche das Management der Geschäftskontinuität (Business Continuity Management) jedoch dem unternehmensweiten Sicherheits- und Risikomanagement. Dementsprechend

ist die Sicherheitspyramide des Autors ein Vorgehensmodell zum Aufbau eines ganzheitlichen Business Continuity Managements (holistic Business Continuity Management {hBCM}).

Wer sich mit dem Business Continuity Management ausschließlich unter dem Teilaspekt Verfügbarkeit beschäftigen möchte, kann das Vorgehensmodell der Sicherheitspyramide beibehalten, wobei er ausschließlich Verfügbarkeits- und Kontinuitätsaspekte betrachtet. Die Sicherheitspyramide heißt dann BCM-/Business-Continuity-Management- bzw. Kontinuitätspyramide nach Dr.-Ing. Müller. Sie bietet den Vorteil, auf Basis des gleichen Vorgehensmodells auch für das Sicherheits- und Risikomanagement erweiterbar zu sein.

Alternative Ansätze und Überlegungen zum BCM finden sich u. a. in der BS 25999-1, den „High-level principles for business continuity“ des Joint Forums des Basel Committee on Banking Supervision sowie im IT Examination Handbook, Business Continuity Planning, des FFIEC.

Kontrollelement – control

Ein Kontrollelement bzw. eine Kontrollaktivität (control activity) dient dazu, die Erreichung eines Kontrollziels nachzuweisen, indem es dieses überwacht und seine Erfüllung sicherstellt. Ein Kontrollelement für den Zutritt bzw. Zugang nur berechtigter Personen erfordert beispielsweise ein Rechtekonzept und einen dokumentierten Berechtigungsvergabeprozess mit ordnungsgemäß unterzeichneten Berechtigungsanträgen und dementsprechend eingerichteten Berechtigungen. Kontrollelemente für den Durchsatz von Prozessen, Systemen und Anlagen sind beispielsweise geeignete Mess- und Überwachungstools, die beim Erreichen vorgegebener Warnschwellen so frühzeitig alarmieren, dass Maßnahmen zur Einhaltung der Kontrollziele noch möglich sind. Darüber hinaus ermöglichen regelmäßige Trendanalysen eine proaktive Vermeidung von Engpässen.

Kontrollziel – control objective

Kontrollziele leiten sich aus den internen und externen Anforderungen sowie SLAs ab. Kontrollziele können beispielsweise sein, dass der Zutritt zum Serverraum und der Zugang zu einer Anwendung nur berechtigten Personen möglich ist, oder dass ein ITK-System oder eine Anlage eine vereinbarte Verfügbarkeit oder einen vereinbarten Durchsatz aufweist.

Kritikalität – criticality

Kritikalität bezeichnet, wie kritisch bzw. wichtig beispielsweise

ein Prozess oder eine Ressource für ein Unternehmen ist.

Kritische IT-Infrastrukturen (KRITIS)

Als Kritische IT-Infrastrukturen (KRITIS) bezeichnet das deutsche BSI „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Zu den kritischen Infrastruktursektoren gehören demzufolge u. a. Transport und Verkehr, Energie, Informationstechnik und Telekommunikation, Finanz-, Geld- und Versicherungswesen, Versorgung, Behörden, Verwaltung und Justiz. [BSI/KRITIS: Der Schutz Kritischer IT-Infrastrukturen in Deutschland, 2005]

Kryptografie – cryptography
s. Verschlüsselung

L**Lightweight Directory Access Protocol (LDAP)**

Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll für den abfragenden oder modifizierenden Zugriff auf Online-Verzeichnisdienste. Im TCP-IP-Protokollstapel (Protocol Stack) ist LDAP auf der Ebene Anwendung angesiedelt. Die 9 RFCs, die die Version 3 des LDAP (LDAPv3) spezifizieren, sind im RFC 3377 zusammengestellt. Hinsichtlich der LDAPv3-Security sind insbesondere der RFC 2251, Lightweight Directory Access Protocol (v3), der RFC 2829, Authentication Methods for LDAP, und der RFC 2830, Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security, von Interesse.

Lokales Netz – Local Area Network (LAN)

Lokale Netze dienen dem internen Hochgeschwindigkeits-Datenaustausch und befinden sich im privaten Besitz des Betreibers. Sie sind beispielsweise in Büros und auf Firmengeländen anzutreffen.

M**MAC**

1. Mandatory Access Control – erzwungene Zugriffskontrolle
2. Medium Access Control – medienspezifisches Zugangsprotokoll
3. Message Authentication Code – Nachrichtenauthentisierung

Maximal tolerierbare Ausfallzeit – Maximum Tolerable Downtime (MTD) / Maximum Acceptable Outage (MAO)

Die maximal tolerierbare Ausfallzeit ist die Zeit, nach der bei einem Ausfall der reguläre oder eingeschränkte Betrieb spätestens wieder aufgenommen worden sein soll. Dies bedeutet, dass innerhalb dieses Zeitraums der Wiederanlauf erfolgreich durchgeführt sein muss.

Maximale Wiederanlaufzeit – Recovery Time Objective (RTO)

Die maximale Wiederanlaufzeit (Recovery Time Objective {RTO}) bezeichnet die Zeit, die benötigt wird, um Schutzobjekte, wie z. B. IT-Systeme und Anwendungen, Räumlichkeiten oder Services nach einem Ausfall wieder verfügbar zu haben.

Mean Time Between Failures (MTBF)

Mean Time Between Failures (MTBF) ist die statistische mittlere Zeitspanne zwischen zwei Fehlern. Die MTBF ist ein Maß für die Zuverlässigkeit von Ressourcen.

Mean Time Between System Incidents (MTBSI)

Mean Time Between System Incidents (MTBSI) ist die statistische mittlere Zeitspanne zwischen zwei Ereignissen (Systemstörungen).

Mean Time To Assist (MTTA)

Mean Time To Assist (MTTA) ist die statistische mittlere Zeitspanne, die zwischen zwei Operatoreingriffen an einer Ressource, z. B. einer Maschine, einer Anlage oder einem System, vergeht.

Mean Time To Repair (MTTR)

Statistische mittlere Reparaturdauer

Mindestgeschäftsbetrieb

Mindestgeschäftsbetrieb bezeichnet den minimal erforderlichen Geschäftsbetrieb zur Aufrechterhaltung der Handlungsfähigkeit eines Unternehmens und zu dessen Überlebenssicherung. Beispielsweise kann in Notfällen oder bei Katastrophen gegebenenfalls eine Zeit lang auf Supportprozesse verzichtet werden, oder Kerngeschäftsprozesse auf die wichtigsten Teilaufgaben beschränkt und mit reduzierter Mitarbeiterzahl durchgeführt werden. Der Mindestgeschäftsbetrieb kann zeitlich gestaffelt sein, d. h. dass er beispielsweise zu Beginn einer Katastrophe am kleinsten ist und im Laufe der folgenden Zeit wieder zunimmt.

Mindestszenarien

Mindestszenarien geben Eckpunkte vor, die bei der Sicherheitsvorsorge bzw. dem Kontinuitätsmanagement, z. B. in Form der Notfall- und Katastrophenvorsorgeplanung, mindestens abzusi-

chern sind. Mindestszenarien sind für alle betrachteten Schutzobjekte erforderlich. Ein Mindestszenario kann beispielsweise der Ausfall eines Rechenzentrums sein. In diesem Fall würde dieser Ausfall bei Vorsorgemaßnahmen berücksichtigt werden müssen, nicht jedoch der gleichzeitige Ausfall zweier Rechenzentren, z. B. des Original- und Ausweichrechenzentrums. Ähnliches gilt, wenn als Mindestszenario der Ausfall eines Gebäudes an einem Standort vorgegeben ist, nicht jedoch der Ausfall mehrerer Gebäude oder des gesamten Standorts.

Mustererkennung – Intrusion Signature Detection

Die Mustererkennung bei Intrusion-Detection-Systemen basiert auf der Annahme, dass sich verschiedene Angriffe anhand charakteristischer Ereignismuster erkennen lassen.

N**Nacharbeit**

Nacharbeit ist in der Regel dann erforderlich, wenn durch den Übergang zum oder vom Notbetrieb sowie im Notbetrieb selbst Leistungen nicht oder nur eingeschränkt erbracht werden konnten. Die liegen gebliebenen Arbeiten sind nachzuarbeiten.

Network Address Translation (NAT)

Durch Network Address Translation (NAT) können IP-Adressen eines (meist internen) Netzes auf die IP-Adressen eines (meist öffentlichen) Netzes übersetzt werden. Hierdurch lassen sich z. B. die internen IP-Adressen gegenüber dem öffentlichen Netz verbergen. Die Umsetzung kann statisch (stets dieselbe Zuordnung) oder dynamisch (Zuordnung erfolgt nach bestimmten Kriterien während der Laufzeit) erfolgen.

Network Attached Storage (NAS)

NAS stellt ein Speichersystem dar, das als (zentraler) Dateiserver dient, und an ein LAN oder WAN angeschlossen ist.

Netzersatzanlage (NEA)

Eine Netzersatzanlage ist eine Stromversorgung in Form eines Notstromaggregats, z. B. Notstromdiesel, mit der ein längerfristiger Stromausfall überbrückt werden kann.

NIST

National Institute of Standards and Technology

Notbetrieb

Unter Notbetrieb wird der vom regulären Betrieb abweichende und in der Regel eingeschränkte Betrieb nach einem Notfall oder einer Katastrophe bezeichnet.

O

Open Authentication (OATH)

Die Open-Authentication-Initiative (OATH) ist eine Arbeitsgemeinschaft führender IT-Unternehmen mit dem Ziel, eine offene Referenzarchitektur für eine universelle starke Authentifizierung zu entwickeln, die sich über alle Nutzer, alle Geräte und alle Netze erstreckt. Ziele sind geringere Kosten für Authentifizierungsgeräte, Interoperabilität, offene Standards, verschiedenartige Authentifizierungsmethoden, wie Einmal-Passwort, SIM-Authentifizierung und PKI-basierende Authentifizierung sowie die Überführung von Handys, PDAs und Notebooks in Geräte mit starker Authentifizierung. Darüber hinaus sollen starke Authentifizierungsalgorithmen und die Authentifizierungssoftware von Clients gemeinsam genutzt werden von Netzendpunkten, wie PCs, Servern, Switches und WiFi-Access-Points.

OpenPGP

OpenPGP, dessen Message Format in RFC 2440 spezifiziert ist, stellt Dienste zur digitalen Signatur und zur Verschlüsselung von Nachrichten, z. B. E-Mails, und Dateien zur Verfügung. OpenPGP basiert auf Pretty Good Privacy (PGP), einer Software-Familie, die von Philip R. Zimmermann entwickelt wurde. Zum Schutz der Vertraulichkeit stellt OpenPGP zwei Verschlüsselungsmethoden zur Verfügung: symmetrische Verschlüsselung und Verschlüsselung mit einem öffentlichen Schlüssel (public key).

Open Systems Interconnection-Referenzmodell (OSI-Referenzmodell)

Das Open Systems Interconnection (OSI)-Referenzmodell der International Organization for Standardization (ISO) wurde als Grundlage für die Bildung von Kommunikationsstandards geschaffen und besteht aus 7 Schichten.

Organization for the Advancement of Structured Information Standards (OASIS™)

Die Organization for the Advancement of Structured Information Standards (OASIS™, www.oasis-open.org) ist eine globale Non-Profit-Organisation, die die Entwicklung, Konvergenz und Anpassung von E-Business-Standards vorantreibt. Sie wurde 1993 unter dem Namen SGML Open als Konsortium von Anbietern und Nutzern gegründet, um Richtlinien für die Interoperabilität zwischen jenen Produkten zu entwickeln, welche die Standard Generalized Markup Language (SGML) unterstützen. 1998 er-

folgte die Umbenennung in OASIS™, um damit das erweiterte Aufgabengebiet zu unterstreichen, das z. B. die Extensible Markup Language (XML) und andere diesbezügliche Standards umfasst.

P

Paketfilter – Packet Filter

Ein Paketfilter führt die Filterung primär auf der OSI-Schicht 3 (Quell- und Zieladresse) der jeweiligen Kommunikationsprotokolle durch sowie gegebenenfalls auf Schicht vier hinsichtlich der Portadressen [71].

Password Authentication Protocol (PAP)

Das Password Authentication Protocol (PAP) ist – wie auch das Challenge-Handshake Authentication Protocol (CHAP) – in RFC 1334 spezifiziert. Es bietet eine einfache Methode zur Benutzerauthentisierung über das Point-to-Point-Protokoll (PPP). PAP überträgt Passwörter unverschlüsselt über das Netz. Ein Schutz vor Playback-Angriffen fehlt. PAP gilt daher als unsicher. CHAP (s. RFC 1994) ist komplexer und überträgt als Antwort auf die Zufallszahl (Challenge) des Servers einen Hashwert, der über einen Einweg-Hash-Algorithmus aus Identifier (Benutzerkennung) und Geheimnis (Passwort) errechnet wurde.

Pharming

Pharming manipuliert die Zuordnung von URL zu IP-Adresse, so dass eine Umleitung auf eine gefälschte Website erfolgt. Angriffsziele beim Pharming sind daher die DNS-Server, aber auch lokale Betriebssystemdateien, in denen diese Zuordnungen gespeichert sind.

Phishing

Phishing ist ein Kunstwort aus „Password fishing“. Es beschreibt eine kriminelle Handlung, bei der Datendiebe versuchen, durch gefälschte E-Mails in den Besitz vertraulicher Daten, wie z. B. PINs, Passwörter, Konto- oder Kreditkartennummern zu gelangen, d. h. vertrauliche Daten „abzufischen“. Die E-Mails sehen Original-Nachrichten von Unternehmen, z. B. Banken, sehr ähnlich. Betätigt der Empfänger den dortigen Link, so gelangt er auf eine gefälschte Webseite, auf der er aufgefordert wird, vertrauliche Daten einzugeben.

Um die Attraktivität derartiger Betrugereien einzudämmen, können z. B. Überweisungslimits dienen. Die Anzeige der zuletzt getätigten Transaktion ermöglicht das Erkennen einer Manipula-

tion beim nächsten Einloggen. Geeignete Challenge-Response-Verfahren mit Einmalpasswörtern können je nach Gegebenheit den Nutzen des Abfischens weiter reduzieren.

PIN – PIN

Persönliche Identifikationsnummer – Personal Identification Number

Sicherheitsmodell - Security Model

Sicherheitsmodelle lassen sich unterscheiden in positive und negative. Positive, auch als „Weiße-Liste“-Modelle (Whitelist Model) bezeichnet, folgen dem Prinzip des generellen Verbots, d. h. sie verbieten alles, bis auf das, was z. B. durch die weiße Liste explizit erlaubt ist. Negative Sicherheitsmodelle, „Schwarze-Liste“-Modelle (Blacklist Model), verhindern nur das, was verboten wurde. Verbote haben jedoch stets die Eigenschaft, dass alles andere erlaubt ist. Ein Beispiel hierfür sind Spam-Mails. Bei einer schwarzen Liste kommt die Spam-Mail durch, sobald die Absenderadresse auf eine nicht gelistete geändert wurde. Bei einer weißen Liste müsste die Spam-Mail demgegenüber eine Absenderadresse haben, die zuvor zugelassen wurde.

Post Office Protocol (POP)

Das Post Office Protocol (POP), Version 3 (POP3), ist in RFC 1939 beschrieben und dient dazu, E-Mails von einem Server auf einen Client herunterzuladen. Die E-Mails werden nach dem Herunterladen auf dem Server gelöscht. POP3 verwendet standardmäßig den TCP-Port 110. POP3-Kommandos bestehen aus ASCII-Zeichen. POP3 überträgt sowohl die E-Mails als auch das Passwort (bei Verwendung des Kommandos PASS) im Klartext.

Die Klartextübertragung des Passworts lässt sich vermeiden, wenn der Server das Kommando APOP implementiert hat. In diesem Fall sendet der Server zu Beginn der Sitzung einen Zeitstempel. Der Client berechnet aus diesem und dem Passwort mittels des MD5-Algorithmus einen Hashwert, den er als Argument des APOP-Kommandos zurückschickt. Gelangt der Server bei seiner Berechnung zum gleichen Hashwert, ist der Authentisierungsvorgang erfolgreich.

Verfügt ein Server über spezielle Erweiterungen, so ist z. B. eine verschlüsselte E-Mail-Übertragung über TLS möglich. Diese Variante heißt POP3s und nutzt den Standard-TCP-Port 995.

POP3 ist funktional geeignet, wenn die E-Mails stets von einem einzigen Client aus abgerufen und lokal verwaltet werden können. Bei Zugriff von unterschiedlichen Rechnern führt dies jedoch dazu, dass die heruntergeladenen E-Mails schließlich über

verschiedene Rechner verteilt sind. Abhilfe schaffen hier IMAP-Server.

Prinzip der minimalen Rechte – Need-to-...-principle

Das Prinzip der minimalen Rechte oder „need-to-...“-Prinzip besagt, dass Subjekte (z. B. Personen) nur die Rechte (z. B. für Zufahrt, Zutritt, Zugang, Zugriff) auf die Objekte (Ressourcen) erhalten, die sie zur Erfüllung ihrer Aufgabe mindestens benötigen.

Prinzip des „aufgeräumten“ Arbeitsplatzes – Clear Desk Policy

Das Prinzip des „aufgeräumten“ Arbeitsplatzes verpflichtet Mitarbeiter, ihren Arbeitsplatz „aufgeräumt“ zu hinterlassen, sodass der Zugang zu Informationssystemen, Datenträgern und Unterlagen für Unbefugte gesperrt ist.

PROSim

Das Akronym PROSim steht für die zweite Dimension der Sicherheitspyramide IV des Autors und repräsentiert die Prozesse, Ressourcen und Organisation für das Sicherheitsmanagement. Je nach Themenstellung lautet das Akronym z. B. bei Kontinuitätsmanagement PROKom bzw. PROBCM, bei Projektmanagement PROProm, bei Qualitätsmanagement PROQuam, bei Risikomanagement PRORim, bei Servicemanagement PROSem, bei Sourcing-Management PROSom, bei Testmanagement PROTem.

Protokollauswertung

Die Protokollauswertung dient der Überprüfung (z. B. durch die Revision) von Protokolldateien, die bei der Protokollierung entstehen.

Protokollierung – logging

Die Protokollierung dient der Aufzeichnung sicherheitsrelevanter Ereignisse, wie z. B. des Zugangs zu Netzen und Systemen oder des Zugriffs auf Daten.

ProTOPSi

Das Akronym ProTOPSi, das die zweite Dimension der Sicherheitspyramide III des Autors repräsentiert, steht für Prozesse, Technologie, Organisation und Personal für Sicherheit. Der Begriff Technologie wurde vom Autor hierbei sehr weit gefasst und bezieht sich u. a. auf Verfahren, Methoden, Werkzeuge und Technik im Sinne von Hardware und Software sowie Infrastruktur, wie z. B. Gebäude. Die Sicherheitspyramide IV fasst die Begriffe Technologie und Personal aus Gründen der Systematik zum umfassenden und verständlicheren Begriff Ressource zusammen.

Public Key Infrastructure (PKI)

Die Public Key Infrastructure ist eine Kombination aus Software,

Verschlüsselungstechnologien und Diensten. Sie unterstützt den Einsatz von Verschlüsselungs- und Signaturdiensten, indem sie die Erstellung, Verteilung, Verwaltung, Prüfung und Rücknahme von Zertifikaten und Schlüsseln regelt.

Public Key Infrastructure (X.509) (PKIX)

Die Arbeitsgruppe Public Key Infrastructure (X.509) der IETF wurde 1995 gegründet. Ihr Ziel bestand in der Entwicklung von Internet-Standards, die eine X.509-basierte PKI unterstützen. Inzwischen entwickelt die Arbeitsgruppe über die ITU PKI-Standards hinaus auch eigene neue Standards zur Nutzung X.509-basierter PKIs im Internet.

R

RADIUS

Remote Authentication Dial In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentisierung und Autorisierung sowie zur Abrechnung (AAA), das in RFC 2865 (RADIUS) und RFC 2866 (RADIUS Accounting) spezifiziert ist. Benutzer, die sich per Modem, ISDN oder DSL an einem Einwahlknoten eines Internet Service Providers (ISP) anmelden, geben zur Identifizierung und Authentisierung üblicherweise ihre Benutzerkennung und ihr Passwort ein. Der Einwahlknoten (Network Access Server {NAS}) fungiert als RADIUS-Client und schickt beides über das RADIUS-Protokoll an den RADIUS-Server. Dieser prüft die Korrektheit der Daten durch Zugriff auf eine Datenbank zugelassener Benutzer. Der RADIUS-Server kann zur Authentisierung beispielsweise das Password Authentication Protocol (PAP) oder das Challenge Handshake Authentication Protocol (CHAP) nutzen. Das Ergebnis der Authentifizierung sendet der Server an den Einwahlknoten zurück.

RAM

1. Ein Random Access Memory (RAM) ist ein Halbleiterspeicher mit kurzen Zugriffszeiten, dessen gespeicherte Informationen bei Abschalten der Betriebsspannung verloren gehen.
2. Reliability, Availability, Maintainability (RAM)

Records Management

Records Management lässt sich im Deutschen mit dem etwas altertümlich anmutenden Begriff Schriftgutverwaltung übersetzen. Records Management dient der Kennzeichnung, Steuerung, Verfolgung und Verwaltung geschäftsrelevanter Unterlagen in Form von physischen und elektronischen Informationen, Dokumenten, Aufzeichnungen und Nachweisen von deren Erstellung

über die Aufnahme, Aufbewahrung, Auffindung, Nutzung und Aussonderung bis hin zur Vernichtung.

Records Management begleitet die Prozesse einer Organisation während ihres gesamten Lebenszyklus. Es beinhaltet u. a. Vorgaben für das Ordnungs- und Ablagesystem, Namenskonventionen für die Identifizierung und Sicherheitsklassifizierung sowie Standards für die Versionierung und Datierung, beginnend mit der Erstell- und später dem Änderungsdatum, über das jeweilige Freigabedatum bis hin zum Aussonderungsdatum. Prozess- und Strukturorganisation mit Zuständigkeiten und Verantwortlichkeiten sind ebenso zu regeln wie Zutritts- und Zugriffs- sowie Bearbeitungsrechte. Die Normenreihe ISO 15489 behandelt das Records Management, das in der deutschen Fassung mit Schriftgutverwaltung übersetzt ist. Als „gute Praxis“ existiert das Good Electronic Records Management (GERM).

Recovery Point Objective (RPO)

Das Recovery Point Objective (RPO) gibt den maximal tolerierbaren Datenverlust in Form des Wiederherstellungszeitpunkts an, also des Zeitpunkts vor einer Störung, für den die Daten wiederherzustellen sind. D.h. er legt fest, wie groß der maximale zeitliche Abstand zu jenem System- und Datenzustand sein darf, der z. B. nach einer Rückspeicherung der Daten wiederherstellbar ist. Werden Daten beispielsweise täglich einmal gesichert, so beträgt der maximale Datenverlust einen Tag, d.h. der Wiederherstellungszeitpunkt liegt maximal einen Tag zurück.

Redundant Array of Inexpensive Disks (RAID)

Ein RAID stellt ein System voneinander unabhängiger Festplatten dar, das zur Erhöhung der Performance und/oder Fehler-toleranz genutzt werden kann. In der ursprünglichen Abkürzung RAID stand „I“ für „Independent“.

Redundanz – Redundancy

Redundanz bezeichnet die „Überfülle“ von Objekten, d. h. deren Duplizität bzw. mehrmaliges Vorhandensein. Beispielsweise können Daten, Informationssysteme, Gebäude, Räumlichkeiten, Arbeitsplätze redundant, also doppelt bzw. mehrfach vorhanden sein, so dass bei Ausfall eines Objektes ein Ersatzobjekt zur Verfügung steht. Redundanz kann näher gekennzeichnet werden durch die Struktur, den Redundanzgrad bzw. die Redundanzquantität, die Redundanzqualität und die Redundanzgeschwindigkeit.

Strukturelle Redundanz ist dann vorhanden, wenn alle Elemente eines Schutzobjektes, d. h. seine Struktur, doppelt bzw. mehrfach

ausgelegt sind.

Die Redundanzquantität gibt an, in welchem Umfang Redundanz besteht. Wird beispielsweise als Ausweichrechenzentrum ein produktives Rechenzentrum mit der gleichen Kapazität wie das Original vorgesehen, also 100%ige Redundanz, so steht bei Ausfall eines Rechenzentrums bei Gleichverteilung jeweils nur noch eine Kapazität von 50 % zur Verfügung.

Die Redundanzqualität ist ein weiteres Charakteristikum der Redundanz. Besteht das duplizierte System aus den gleichen Komponenten, so kann der z. B. alterungs- oder umfeldbedingte Ausfall eines Systems abgefangen werden, nicht jedoch systembedingte. Systembedingte Fehler können dann zusätzlich abgefangen werden, wenn das zweite System die gleiche Funktionalität wie das Original aufweist, aber z. B. von einem anderen Hersteller stammt, so dass der gleiche systembedingte Fehler wahrscheinlich nicht auftritt. Die Redundanzqualität ist in diesem Fall höher. Diese Ausführungen gelten in analoger Form für alle Ressourcen, z. B. auch für externe Dienstleister.

Die Redundanzgeschwindigkeit, d. h. die Geschwindigkeit mit der das redundante System vollständig oder etappenweise zur Nutzung zur Verfügung gestellt werden kann, ist ein weiterer Aspekt der Redundanz. Redundanzgeschwindigkeit nenne ich dies deshalb, weil die Ersatz-Schutzobjekte, die ein Gesamtsystem ersetzen sollen, oftmals erst nach und nach in Betrieb gehen.

Resilience

(Fault oder Failure) Resilience, d. h. Fehlerelastizität bzw. Fehler-toleranz, bezeichnet die Eigenschaft eines Unternehmens, eines Prozesses, einer Ressource, eines Produktes oder einer Dienstleistung, sich trotz einer begrenzten Anzahl von Fehlern weiterhin anforderungs- bzw. spezifikationsgerecht zu verhalten, eventuell auf einem akzeptierten minimalen Leistungsniveau.

Return on Safety, Security and Continuity Investment (RoSSCI)

Als Return on Safety, Security and Continuity Investment (RoSSCI) bezeichnet der Autor den Ertrag und den vermiedenen Schaden, den ein Unternehmen aufgrund von Investitionen hat, welche es in die Betriebs- und Angriffssicherheit sowie die Kontinuität getätigt hat.

Return on Security Investment (RoSI)

Return on Security Investment bezeichnet den Ertrag und den vermiedenen Schaden, den ein Unternehmen aufgrund einer in die Sicherheit getätigten Investition hat.

Risikoanalyse – Risk Analysis

Risikoanalyse ist der Prozess zur Ermittlung, Analyse und Bewertung von Sicherheitsrisiken sowie zur Identifikation zusätzlich erforderlicher Sicherheits- und Kontinuitätsmaßnahmen.

Risikomanagement – Risk Management

Risikomanagement ist der Prozess zur Identifizierung, Bewertung und Steuerung sowie Vermeidung, Verringerung, Verlagerung oder Vereinnahmung (Akzeptanz) von Risiken.

Risikostrategie – Risk Strategy

Die Risikostrategie für ein einzelnes Risiko kann ausgerichtet sein auf Vermeidung, Verringerung, Verlagerung oder Vereinnahmung (Akzeptierung) des Risikos.

Role Based Access Control (RBAC)

Role Based Access Control (RBAC) [100], also rollenbasierte Zugriffskontrolle, ist als ANSI-Norm definiert und enthält ein Referenzmodell mit den dazugehörigen funktionalen Spezifikationen. Das Referenzmodell definiert RBAC-Elemente, wie z. B. Benutzer, Rollen, Berechtigungen und Objekte.

Am 1. Februar 2005 wurde der OASIS™-Standard „Core and hierarchical role based access control (RBAC) profile of XACML v2.0“ verabschiedet. Er definiert ein XACML-Profil, um die Anforderungen an „core“ und „hierarchical“ RBAC zu erfüllen, wie sie in der ANSI-Norm spezifiziert sind.

S

Schutzbedarfsanalyse – Business Impact Analysis

Die Schutzbedarfsanalyse ermittelt die Sicherheitsanforderungen je Sicherheitskriterium anhand der Auswirkungen, die sich bei einer Beeinträchtigung des jeweiligen Sicherheitskriteriums ergeben. Beispielsweise erhebt sie, welche Auswirkung der Ausfall eines Gebäudes oder eines Informationssystems auf den Geschäftsprozess hat. Nach der Ermittlung der Schadenshöhe erfolgt je Sicherheitskriterium die Einstufung in eine Sicherheitsklasse. Im Rahmen der Schutzbedarfsanalyse wird auch der zeitlich gestaffelte Mindestgeschäftsbetrieb erhoben.

Schutzobjekt

Prozesse nutzen Ressourcen. Eine Störung, eine Kompromittierung oder ein Ausfall dieser Ressourcen oder des Prozesses selbst kann die Funktionsfähigkeit der Geschäftsprozesse beeinträchtigen oder sie komplett ausfallen lassen. Daher bezeichne ich alle Ressourcen,

die von einem Prozess genutzt werden, sowie den Prozess selbst, als Schutzobjekte. Schutzobjekte sind die konkrete Ausprägung einer Schutzobjektklasse. Das <Musterinformationssystem> ist z. B. eine konkrete Ausprägung der Schutzobjektklasse Informationssystem.

Schutzobjektklasse

Schutzobjektklassen fassen konkrete Schutzobjekte eines bestimmten Typs unter einem gemeinsamen Oberbegriff zusammen. Die Schutzobjektklasse Informationssysteme repräsentiert beispielsweise alle in einem Unternehmen eingesetzten konkreten Informationssysteme. Zu den Schutzobjektklassen gehören u. a. Prozesse, Gebäude, Räumlichkeiten, räumliche und haustechnische Infrastruktur, Informations- und Kommunikationssysteme, Daten, Hilfs- und Arbeitsmittel, Anlagen, Fertigungsstraßen, Materialien, finanzielle Mittel, Services und nicht zuletzt Personen sowie Know-how und Image.

Schutzobjektklassen lassen sich üblicherweise durch ähnliche Sicherheitsmaßnahmen schützen. Dies vereinfacht und standardisiert das Repertoire an Sicherheitsmaßnahmen.

Schwachstelle

Eine Schwachstelle stellt eine Sicherheitslücke oder ein Sicherheitsdefizit dar.

Secure Socket Layer (SSL)

Der Secure Socket Layer sichert WWW-Verbindungen durch Verschlüsselung.

Sensibilisierung

Sensibilisierung für das Thema Sicherheit dient dazu, bei Mitarbeitern Bewusstsein für Sicherheitsanforderungen, Bedrohungen, Schwachstellen, Risiken und Sicherheitsmaßnahmen zu schaffen.

Serial Attached SCSI (SAS)

Serial Attached SCSI stellt laut der SCSI Trade Association eine Weiterentwicklung von SCSI dar. Hierbei findet ein Übergang von der parallelen auf eine serielle Schnittstelle statt. Die erste Generation mit einer Übertragungsrate von 3Gb/s, ersetzt das parallele SCSI, das die Leistungs- und Skalierbarkeitsanforderungen der Industrie nicht mehr erfüllt. Die nächste SAS-Stufe sieht eine Übertragungsrate von 6Gb/s vor.

Service-Vereinbarung – Service Level Agreement (SLA)

Eine Service-Vereinbarung (Service Level Agreement {SLA}) beinhaltet die messbare Festlegung der zwischen Service-Geber und Service-Nehmer vereinbarten Leistungen.

Sicherheitskonzept – Safety/Security Specification

Ein Sicherheitskonzept legt fest, welche Maßnahmen zur Erhö-

hung der Sicherheit für ein spezifisches Thema oder Objekt, z. B. ein IT-System, ein Netz oder eine Anwendung, ergriffen werden sollen.

Sicherheitskriterien – Safety/Security Criteria

Unter Sicherheitskriterien versteht der Autor Konformität, Robustheit, Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit und Authentizität sowie die sekundären Sicherheitskriterien Nachvollziehbarkeit, Nachweisbarkeit, Erkennungs-, Alarmierungs- und Abwehrfähigkeit.

Sicherheitsleitlinien – Safety/Security Guidelines

Sicherheitsleitlinien geben einen Orientierungsrahmen für die Sicherheit im Unternehmen.

Sicherheitsmanagement – Safety/Security Management

Das Sicherheitsmanagement beinhaltet die systematische Planung, Umsetzung, Steuerung und Weiterentwicklung der Sicherheit im Unternehmen oder in Organisationseinheiten. Ein durchgängiges, effizientes und praxisorientiertes Vorgehensmodell für das integrative Sicherheits-, Kontinuitäts- und Risikomanagement in Unternehmen bietet die in diesem Buch dargestellte dreidimensionale Sicherheitspyramide nach Dr.-Ing. Müller. Sie umfasst die Sicherheitshierarchie, die IT-Prozesse einschließlich des IT-Sicherheitsmanagementprozesses, die Ressourcen und die Organisation bis hin zum Lebenszyklus von Prozessen, Ressourcen, Produkten und Dienstleistungen sowie das Monitoring und Controlling mit entsprechenden Kennzahlen.

Verschiedene Normen und Practices bieten alternative Vorgehensweisen. Sie konzentrieren sich auf unterschiedliche Themen und unterscheiden sich in den Abstraktionsebenen, die derzeit verschiedentlich noch überblicksartig sind. Dementsprechend weisen sie unterschiedliche Ansätze und Stärken auf. Die Herausforderung für den Praktiker besteht darin, diese verschiedenen Ansätze und Stärken zusammenzuführen.

Die Sicherheitspyramide nach Dr.-Ing. Müller vereinigt seit vielen Jahren Ansätze, die in unterschiedlicher Tiefe und Ausprägung sowie verstreut auch in Normen und Practices enthalten sind. Im ITK-Bereich gehören zu diesen Normen und Practices die ISO 13335-1:2004, die ISO 17799:2005, die ISO 27001:2005, ITIL® und COBIT® sowie das IT-GSHB des BSI und die Balanced Scorecard. Im Hinblick auf das Kontinuitätsmanagement bezieht sich dies u. a. auf den Standard BS 25999-1:2006.

Sicherheitsmaßnahme – Safeguard bzw. Safety/Security Measure

Maßnahme, Mechanismus, Prozess oder Schutzsubjekt zur Ver-

meidung, Verringerung oder Verlagerung eines Risikos bzw. zur Steigerung des Sicherheitsniveaus.

Sicherheitsniveau – Safety/Security Level

Das Sicherheitsniveau beschreibt das Maß an Sicherheit.

Sicherheitsphilosophie – Safety/Security Philosophy

Die Sicherheitsphilosophie legt in schriftlicher überblicksartiger Form fest, welche Bedeutung und Ausprägung das Thema Sicherheit haben soll.

Sicherheitspyramide – Safety/Security Pyramid

Die Sicherheitspyramide nach Dr.-Ing. Müller stellt ein anschauliches, strategisches, systematisches und ganzheitliches Vorgehensmodell zum schrittweisen Aufbau und zur Weiterentwicklung des Sicherheits-, Kontinuitäts- und Risikomanagements dar. Sie ist hierarchisch aufgebaut und berücksichtigt den Lebenszyklus von Prozessen und Ressourcen, wie z. B. (ITK-) Systemen, sowie Produkten und Dienstleistungen hinsichtlich der Themenfelder Prozesse, Ressourcen und Organisation und im Hinblick auf das Sicherheitsmanagement (PROSim).

Sicherheitsrichtlinien – Safety/Security Guidelines

Sicherheitsrichtlinien geben einen einzuhaltenden Rahmen vor.

Sicherheitsstandards – Safety/Security Standards

Sicherheitsstandards geben – wie auch Sicherheitsrichtlinien – einen einzuhaltenden Rahmen vor.

Sicherheitsstrategie – Safety/Security Strategy

Die Sicherheitsstrategie legt fest, welches Maßnahmenbündel von der Prävention über die Detektion und Meldung bzw. Alarmierung sowie der Reaktion bis hin zur Wiederherstellung zur Vermeidung, Verringerung oder Verlagerung eines Risikos in welchem Umfang ergriffen werden sollte.

Sicherheitsstudie – Safety/Security Study

Eine Sicherheitsstudie beinhaltet den Prozess zur Ermittlung, Analyse und Bewertung von Risiken sowie zur Identifikation zusätzlich empfohlener oder erforderlicher Sicherheitsmaßnahmen.

Sicherheits-, Kontinuitäts- und Risikopolitik – Safety/Security, Continuity and Risk Policy

In der Sicherheits-, Kontinuitäts- und Risikopolitik eines Unternehmens legt die Unternehmensleitung in schriftlicher überblicksartiger Form fest, welche Bedeutung und Ausprägung das Thema Sicherheit und Kontinuität für das Unternehmen haben soll und äußert sich zur Risikostrategie und -tragfähigkeit.

Sicherheitsziele – Safety/Security Objectives

Sicherheitsziele leiten sich aus der Sicherheits- und Risikopolitik ab und werden im Rahmen einer Schutzbedarfsanalyse anhand von Schadensszenarien und deren Konsequenzen ermittelt.

Simple Mail Transfer Protocol (SMTP)

Das Simple Mail Transfer Protocol (SMTP) ist ein E-Mail-Dienst, welcher der Übertragung von E-Mails dient. Es ist beschrieben in RFC 2821 und basiert auf der ursprünglichen Spezifikation in RFC 821.

Single Point of Failure (SPoF)

Ein „Single Point of Failure“ (Einzelfehler) ist eine Stelle, an der ein einzelner Fehler zu einem Ausfall führt. Derartige Situationen ergeben sich bei nicht konsequent redundanter Auslegung von Ressourcen.

Single Sign-on

Das Single Sign-on dient dazu, mit nur einem Identifikations- und Authentisierungsvorgang Zugang zu verschiedenen Systemen zu erhalten. Dies gilt in entsprechender Form für den Zutritt zu verschiedenen Gebäuden oder Räumlichkeiten.

Skript Kiddie

Die Bezeichnung Skript Kiddie kennzeichnet Internet-Nutzer, die Angriffe unter Nutzung vorgefertigter Schadprogramme durchführen. Daher reichen für ihre Angriffe bescheidene technische Kenntnisse aus. Ihre Attacken erfolgen meist wahllos und nicht zwangsläufig zur vorsätzlichen Schädigung der Angegriffenen, sondern entspringen teilweise der Neugier z. B. jugendlicher Internet-Nutzer.

Small Computer System Interface (SCSI)

Das Small Computer System Interface (SCSI) bezeichnet eine standardisierte parallele Schnittstelle zur Verbindung der Prozessoreinheit des Computers mit Peripheriegeräten, z. B. Festplatten. Sie ermöglicht in der einfachen Form den Anschluss von bis zu 8 und in erweiterter Form von bis zu 16 Geräten. (Wide) Ultra320 SCSI erlaubt eine max. Übertragungsgeschwindigkeit von 320 MByte/s bei einer Busbreite von 16 Bit.

Sniffer

Ein Sniffer ist ein Programm, das Datenpakete, die über ein Netz übertragen werden, heimlich mitliest.

Social Engineering

Beim Social Engineering bringt ein Angreifer sein Opfer dazu, Dinge zu tun, die der Angreifer will. So gibt sich ein Angreifer

z. B. als Netzadministrator oder Sicherheitsmanager aus und erschleicht sich unter einem Vorwand Passwörter. Meist erfolgen diese Angriffe per Telefon, da es so schwieriger ist, des Täters habhaft zu werden. Aber auch entsprechendes Auftreten kann zum unberechtigten Zutritts- und Zugangserfolg führen, genauso wie der Auftritt als vermeintlicher Repräsentant eines Herstellers und „bewaffnet“ mit entsprechender Hardware. Phishing ist ebenfalls ein Beispiel für Social Engineering.

Speichernetz – Storage Area Network (SAN)

Speichernetze verbinden Speichereinheiten untereinander und mit Computern.

Spionagesoftware – Spyware

Spionagesoftware sind Programme, die mit oder ohne das Wissen des Nutzers auf seinem Computer installiert werden, Informationen sammeln und weiterleiten. Sie können damit die Privatsphäre beeinträchtigen. Spyware kann z. B. in kostenloser Software enthalten sein oder beim Besuch von Webseiten heruntergeladen werden. Spionagesoftware verlangsamt den Rechner.

Structured Query Language (SQL)

Die Structured Query Language (SQL) ist eine datenbank-unabhängige Sprache, welche die Definition von Datenstrukturen und die Operationen auf diese beschreibt. SQL ist in der Normenreihe ISO/IEC 9075 festgelegt. SQL ist unterteilt in die Data Definition Language (DDL), die Data Manipulation Language (DML), die Data Query Language (DQL) und die Data Control Language (DCL). DDL enthält die Befehle CREATE, ALTER, DROP, DML die Befehle INSERT, UPDATE, DELETE, DQL den Befehl SELECT und DCL die Befehle GRANT und REVOKE.

SQL-Injektion – SQL Injection

SQL-Injektion bezeichnet eine Angriffsmethode auf Datenbanken, bei der ein Angreifer die fehlende Plausibilisierung der Parameterein- oder -übergabe an ein SQL-Statement ausnutzt und auf diese Weise das SQL-Statement manipuliert. Plausibilisierungen sollten sich auf die Feldinhalte und die Feldlänge beziehen.

Zur Manipulation eines SQL-Statements können Angreifer folgende SQL-Elemente nutzen:

- den SQL String Delimiter ('),
- den SQL Statement Concatenation Character (;) und
- die SQL Comment Sequence bzw. Character nutzen (bei Microsoft® SQL Server: --, bei MySQL: #).

Als prinzipielles Beispiel dient die folgende SQL-Abfrage:

```
SELECT * FROM benutzertabelle WHERE benutzername = '$uid'  
AND passwort = '$pwd'
```

Diese Abfrage soll prüfen, ob der eingegebene Benutzername zusammen mit dem Passwort in der Benutzertabelle vorhanden sind, es sich also um einen zugelassenen Benutzer handelt.

Ein Angreifer könnte für die abgefragten Parameter folgende Eingaben verwenden:

Für \$uid eine beliebige Eingabe, z.B. abc

Für \$pwd die Eingabe ' OR 2=2 --

Übernimmt das Programm die Eingaben ungeprüft, so resultiert hieraus die Abfrage

```
SELECT * FROM benutzertabelle WHERE benutzername = 'abc'  
AND passwort = '' OR 2=2 --'
```

Da 2=2 immer richtig ist und der Rest der Abfrage aufgrund der beiden Striche als Kommentar gekennzeichnet ist, liefert diese Abfrage stets das Ergebnis „richtig“, womit der Angreifer als berechtigter Nutzer identifiziert und authentifiziert wäre.

Statement on Auditing Standards (SAS) No. 70

Das Statement on Auditing Standards (SAS) No. 70, Service Organizations, repräsentiert einen Prüfungsstandard des AICPA (American Institute of Certified Public Accountants). Durch SAS No. 70 können Dienstleistungsunternehmen ihre internen Kontrollaktivitäten und -prozesse einer Prüfung durch einen Wirtschaftsprüfer unterziehen. Das Ergebnis ist ein formaler Bericht in einem typischerweise einheitlichen Format, den das Dienstleistungsunternehmen seinen Kunden und deren Prüfern zur Verfügung stellen kann. Wenn die Kunden diesen Bericht akzeptieren, lassen sich die jährlich vielfältigen Prüfungen der verschiedenen Kunden auf eine jährliche Prüfung des Wirtschaftsprüfers reduzieren. Dadurch lassen sich sowohl beim Dienstleister als auch beim Kunden Prüfungszeiten einsparen.

SAS No. 70 ist für jene Kunden interessant, die Aspekte, die für die Rechnungslegung relevant sind, an Dienstleister ausgelagert haben. Dies trifft insbesondere auch dann zu, wenn die Kunden hinsichtlich der Rechnungslegung dem Sarbanes-Oxley Act (SOX) unterliegen. Das AICPA unterscheidet SAS No. 70 nach Typ I und Typ II.

Bei SAS No. 70 Typ I äußert sich der Auditor dazu, ob die vom Dienstleister angegebenen Kontrollaktivitäten in angemessener Form dessen wesentlichen operativen Kontrollaktivitäten widerspiegeln. Weiterhin beurteilt er, ob die Kontrollaktivitäten angemessen sicherstellen, dass bei ihrer Anwendung die Kontrollziele

eingehalten werden.

Bei SAS No. 70 Typ II trifft der Auditor darüber hinaus eine Aussage dazu, ob die getesteten Kontrollaktivitäten hinreichend effektiv arbeiten und erwarten lassen, dass die Kontrollziele während des angegebenen Zeitraums erreicht wurden.

Steganografie – Steganography

Steganografie bedeutet, abgeleitet aus dem Griechischen, „verstecktes Schreiben“. Sie bezeichnet eine Methode, mit der Nachrichten unbemerkt übermittelt werden können, indem Nachrichten z. B. in digitalen Grafiken, Bildern, Filmen oder Musik versteckt werden.

T

Taschenauthentifikator – Token

Der Taschenauthentifikator besteht häufig aus einer Anzeige sowie einem Eingabefeld und verfügt über einen geheimen Schlüssel sowie gegebenenfalls eine interne Uhr. Er dient dazu, ein Einmal-Passwort zu erzeugen.

Test – Test

Ein Test dient der Überprüfung, ob die Anforderung, die an ein Prüfobjekt gestellt wurden, erfüllt werden.

Transaktionsnummer (TAN) – Transaction Number

Eine Transaktionsnummer (TAN) dient der Autorisierung einer Transaktion. Sie wird beispielsweise bei der Autorisierung einer Banküberweisung über das Internet eingesetzt. Beim Basis-TAN-Verfahren wählt der Kunde eine TAN aus einer Liste aus und autorisiert damit die Transaktion.

Zum stärkeren Schutz gegenüber betrügerischen Aktivitäten, z. B. in Form von Phishing, geben Banken zur Autorisierung einer Transaktion die Nummer derjenigen TAN aus der TAN-Liste vor, die der Kunden eingeben soll. Dieses Verfahren verwendet somit „indizierte TANs“ (iTAN) und erschwert die Nutzung einer „abgefischten“ TAN.

Das iTAN-Verfahren schützt nicht vor „man-in-the-middle-Attacken“. Betrüger locken hierbei das potenzielle Opfer – beispielsweise über einen Link in einer Phishing-E-Mail – auf die von ihnen gefälschte Website. Hier fordern sie die Eingabe der Kontonummer und PIN. Erhalten sie diese Informationen, bauen sie eine Verbindung zur Bank auf. Hat das Opfer seine Transaktion eingegeben, manipuliert der Angreifer die Daten und schickt sie an das Finanzinstitut. Die Bank fordert daraufhin eine iTAN

an. Diese Aufforderung leitet der Betrüger an den Kunden weiter. Dessen Eingabe gibt der Angreifer zur Autorisierung der gefälschten Transaktion an das Bankinstitut weiter.

Alternativ zum iTAN-Verfahren existiert das mobile TAN-Verfahren (mTAN). Zur Autorisierung der Transaktion erhält der Nutzer die TAN per SMS auf sein Handy. Diese Einmal-TAN ist nur für die jeweilige Transaktion gültig. Werden mit der TAN per SMS gleichzeitig die Transaktionsdaten, also Empfängerkonto, Empfängerbank und Betrag, übermittelt, kann der Benutzer eine „man-in-the-middle-Attacken“ entdecken. Voraussetzung ist hierbei – wie auch beim Phishing – die Sensibilisierung des Nutzers, damit er die übermittelten Daten einschließlich des Absenders genau prüft. Außerdem sollte er im Hinblick auf einen Handy-Diebstahl oder -Verlust seine eigene Kontonummer und PIN nicht auf dem Handy oder Smartphone speichern. Auch bei der Weitergabe der Handy-Nummer kann Vorsicht angeraten sein, nicht zuletzt, wenn diese per Phishing abgefragt wird. Gleichzeitig nimmt durch die mobile TAN der Schutzbedarf des Handys und gegebenenfalls des mobilen Nutzers zu. Auch hier empfiehlt sich eine Pfadanalyse, um das Sicherheitsniveau aller beteiligten Elemente und die möglichen Angriffsszenarien zu ermitteln.

Beim eTAN-Verfahren erhält der Kunde eine PIN und ein Gerät, den TAN-Generator. Die Autorisierung einer Transaktion läuft über ein Challenge-Response-Verfahren: Der Computer der Bank erzeugt eine Kontrollnummer (Challenge) und übermittelt sie an den Kunden. Der Kunde gibt sie in seinen TAN-Generator ein. Der TAN-Generator erzeugt eine Antwortnummer (Response), mit der der Kunde die Transaktion autorisiert.

Alternativ hierzu existieren TAN-Generatoren, die eine TAN erzeugen, die nur eine begrenzte Zeit lang gültig ist.

Für das eTAN-Plus-Verfahren bekommt der Kunde eine PIN, einen speziellen mobilen Kartenleser mit Tastatur und eine Chipkarte. Zur Autorisierung einer Transaktion steckt der Kunde seine Chipkarte in den Kartenleser ein und tippt die vom Bankcomputer erzeugte Nummer (Challenge) ein. Der Kartenleser berechnet aus den Transaktionsdaten und dem geheimen Schlüssel in der Chipkarte die TAN (Response) und zeigt sie im Display an. Hiermit autorisiert der Kunde die Transaktion mit den spezifischen Transaktionsdaten.

Weitere Schutzmaßnahmen bestehen darin, Datum und Uhrzeit des letzten Login sowie im Falle der PIN- oder TAN-Eingabe am Bildschirm einen Ziffernblock anzuzeigen. Der Ziffernblock kann per Maus angeklickt werden, um die Ziffern nicht per Tastatur

einzugeben und so ein „Abhören“ der Transaktionsnummer zu erschweren. Außerdem kann bei der PIN-TAN-Eingabe vom Benutzer zusätzlich die Eingabe von Buchstaben und Ziffern gefordert werden, die auf dem Bildschirm verzerrt, gekippt und/oder versetzt auf grauem Hintergrund angezeigt werden. Diese sind für den Menschen leicht, für Malware aber schlechter zu erkennen. Dies erschwert automatisierte Angriffe, z. B. solcher DoS-Attacken, die das Ziel haben, durch Eingabe beliebiger Kontonummern und jeweils mehrmaliger falscher PIN-Eingabe Konten zu sperren.

Transport Layer Security (TLS)

Das Transport-Layer-Security-Protokoll, vormals bekannt als SSL, ist in der Version 1.0 in RFC 2246 spezifiziert, in Verbindung mit IMAP, POP3 und ACAP in RFC 2595. TLS dient dem Schutz gegen Abhören und unzulässige Veränderung (Integrität) durch Verschlüsselung. TLS besteht aus zwei Ebenen: dem TLS Record Protocol und dem TLS Handshake Protocol. Das TLS Record Protocol dient der Verbindungssicherheit und der Kapselung verschiedener darüber liegender Protokolle, wie z. B. des TLS Handshake Protocol. Letzteres ermöglicht es dem Server und dem Client, sich gegenseitig zu authentisieren sowie einen Verschlüsselungsalgorithmus und Schlüssel auszuhandeln. TLS befindet sich im TCP/IP-Protokoll-Stack zwischen dem Transport Layer mit TCP und der Anwendungsschicht (application layer) mit http, LDAP, SMTP, Telnet etc.

Trojanisches Pferd – Trojan Horse

Ein trojanisches Pferd in der ITK ist – in Analogie zur List des Odysseus im Kampf um Troja – Programmcode, der etwas Nützliches zu tun vorgibt, während er tatsächlich etwas Unerwünschtes ausführt. Beispielsweise kann es Programmcode sein, der die Login-Maske darstellt und Benutzerkennung und Passwort dann an Unbefugte weiter leitet.

U

Übung – practice

Eine Übung dient dazu, ein Verfahren oder eine Vorgehensweise durch ihre (regelmäßige) Anwendung geläufig zu machen.

Universal Business Language (UBL)

OASIS™ hat im Dezember 2006 die Universal Business Language (UBL), Version 2.0 als OASIS™-Standard freigegeben. UBL definiert eine XML-Bibliothek für Geschäftsdokumente und ist die

erste Standard-Implementierung der Electronic business eXtensible Markup Language (ebXML) Core Components Technical Specification 2.01. UBL zielt darauf ab, in einem Standard-Geschäftsrahmenwerk wie z. B. ISO/TS 15000 (ebXML) zu arbeiten. Die UBL-Bibliothek besteht aus Informationskomponenten, den Business Information Entities (BIE). Eine Datenkomponente ist beispielsweise die „Adresse“, die in verschiedenen Dokumententypen vorkommt. BIEs lassen sich zu spezifischen Dokumententypen zusammensetzen, wie z. B. einem Auftrag oder einer Rechnung. [101]

Unterbrechungsfreie Stromversorgung (USV) – Uninterruptable Power Supply (UPS)

Eine USV ist eine Stromversorgung, mit der ein kurzzeitiger Stromausfall überbrückt werden kann. Die IEC 62040-3 nennt folgende 10 Netzstörungen: 1. Netzausfälle, 2. Spannungsschwankungen, 3. Spannungsspitzen, 4. Unterspannungen, 5. Überspannungen, 6. Blitzeinwirkung, 7. Spannungsstöße, 8. Frequenzschwankungen, 9. Spannungsverzerrungen, 10. Spannungsüberschwingungen. Die IEC 62040-3 unterscheidet folgende USV-Klassen:

- Voltage and Frequency Independent (VFI) from mains supply. Dieser USV-Typ ist vergleichbar mit der Online-USV mit Dauerwandler. Bei VFI-USVs sind Spannung und Frequenz am USV-Ausgang unabhängig vom Eingangsnetz. VFI-USVs bieten Schutz gegen alle 10 Netzstörungsarten. Bei einer VFI-USV läuft die Stromversorgung der angeschlossenen Geräte, z. B. Computer, stets über die USV.
- Voltage Independent (VI) from mains supply. Diese USV-Klasse ist vergleichbar mit Line-Interactive-USVs. Bei VI-USVs ist die Spannung am USV-Ausgang unabhängig vom Eingangsnetz. Störungen der Netzfrequenz gelangen ungefiltert zur Last. VI-USVs bieten Schutz gegen die Netzstörungsarten 1 – 5. Sie überbrücken Stromausfall und können Spitzen und Unebenheiten in der Stromversorgung glätten.
- Voltage and Frequency Dependent (VFD) from mains supply. VFD-USVs sind vergleichbar mit Offline-USVs. Eine VFD-USV befindet sich solange im „standby“-Modus wie das Netz die Last im regulären Betrieb direkt versorgt. Erst im Falle einer Störung der Stromversorgung erfolgt die Umschaltung auf den Batteriebetrieb. VFD-USVs bieten Schutz gegen die Netzstörungsarten 1 – 3.

Als Kennzeichnung für USVs enthält die Norm darüber hinaus weitere Angaben. Der Bezeichnung der USV-Klasse folgen zwei Buchstaben. Diese charakterisieren die Form der Spannungskur-

ve am USV-Ausgang im Normalbetrieb (1. Buchstabe) und im Batteriebetrieb (2. Buchstabe). Angestrebt ist eine reine Sinuskurve. Als Buchstaben sind S, X und Y möglich. Der Buchstabe S repräsentiert die Bestmarke. Bei Y, dem schlechtesten Wert, ist die Wellenform nicht sinusförmig und der Klirrfaktor vom Hersteller zu spezifizieren.

Der anschließende dreistellige Code kennzeichnet das dynamische Spannungsverhalten am USV-Ausgang: 1. bei Änderungen der Betriebsart, 2. bei Zu- und Abschalten einer linearen sowie 3. einer nichtlinearen Referenzlast. Die Skala reicht vom besten Wert 1 für USVs, die „für alle Arten von Belastungen geeignet sind“ bis zum schlechtesten Wert 3. Den höchsten Schutz bietet daher eine VFI-SS-111. Unter Kontinuitätsaspekten ist zu berücksichtigen, dass die USV einen SpoF darstellen kann. Sie sollte daher in geeigneter Form redundant ausgelegt sein.

Unverfälschtheit (Integrität) – Integrity

Eigenschaft eines Objekts, unverfälscht und vollständig, d. h. nicht unzulässig oder unbefugt verändert oder gelöscht worden zu sein.

V

Validierung – Validation

Die Validierung prüft die Übereinstimmung des erzeugten Produktes bzw. der erbrachten Leistung mit den Anforderungen der Auftraggeber. Dies beinhaltet die Überprüfung der Sicherheitsanforderungen. Ein Beispiel ist die Überprüfung, dass ein Software-Produkt die Anforderungen der Benutzer erfüllt.

Verbindlichkeit (Nichtabstreitbarkeit) – (non repudiation)

Eigenschaft eines Objekts, z. B. einer Transaktion, verbindlich, d. h. nicht abstreitbar zu sein.

Vereinzelungsanlage

Der Zutritt zu Räumlichkeiten mit einem sehr hohen Schutzbedarf ist meist über Vereinzelungsanlagen gesichert, so dass nur eine einzelne Person mit entsprechenden Zutrittsrechten in den jeweiligen Raum gelangen kann. Die Ausführungen derartiger Personenvereinzelungsanlagen reichen von Schleusen, z. B. Rund- und Schiebetürschleusen, bis hin zu Vereinzelungs-Drehtüren.

Darüber hinaus existieren automatische videobasierte Personenvereinzelungssysteme, die auf der Silhouettenerkennung (Schattenriss) beruhen, und in bestehenden Räumlichkeiten genutzt werden können. Sie ermöglichen eine Mehrpersonenvereinzelung

und eine Leerraumdetektion, durch die absichtlich oder unabsichtlich zurückgelassene Objekte erkannt und gemeldet werden können. Derartige Systeme eröffnen – nach Abgleich der Sicherheitsanforderungen mit den Bedrohungen – prinzipiell die Möglichkeit, zutrittsgeschützte Bereiche, z. B. Schließfachbereiche, zu automatisieren sowie eine Korridor- und Vorraumüberwachung hochkritischer zutrittsgeschützter Bereiche vorzunehmen.

Verfügbarkeit – Availability

Eigenschaft eines Objekts, wie z. B. eines Prozesses oder einer Ressource (Gebäude, Räumlichkeiten, Computer, Netze, Personen, Daten, ...), in einem bestimmten Umfang bereit zu stehen, zugreifbar und nutzbar zu sein.

Verfügbarkeitsklassen – Availability Environment Classification (AEC)

Die Harvard Research Group hat Verfügbarkeit in 5 Klassen von 0 bis 4 definiert (Availability Environment Classification {AEC}) [102]. Diese orientieren sich an den Auswirkungen eines Ausfalls auf die Geschäftsaktivitäten und auf die Kunden. Die Klassen enthalten folgende Charakteristika:

- AE4 – Rund-um-die-Uhr-Betrieb, d. h. 24 h x 7 Tage. Die Geschäftsfunktionen erfordern kontinuierliche Verfügbarkeit, ein Ausfall wäre für den Nutzer transparent.
- AE3 – Unterbrechungsfreier Betrieb entweder während wesentlicher Zeiträume oder während des überwiegenden Teils des Tages, der Woche und des Jahres. Der Nutzer bleibt online. Ein Restart der aktuellen Transaktion kann jedoch erforderlich sein und Performance-Einbußen können auftreten.
- AE2 – Betrieb mit minimalen Unterbrechungen entweder während wesentlicher Zeiträume oder während des überwiegenden Teils des Tages, der Woche und des Jahres. Der Benutzer wird unterbrochen, kann sich jedoch zeitnah wieder einloggen. Transaktionen müssen gegebenenfalls unter Nutzung von Aufzeichnungsdateien wiederholt werden und es können Performance-Einbußen auftreten.
- AE1 – Betrieb mit Unterbrechungen, jedoch mit Verfügbarkeit der Daten. Der Benutzer kann nicht weiterarbeiten, das System fährt unkontrolliert herunter. Eine Datensicherung auf einer redundanten Festplatte liegt vor. Unter Nutzung von Log- oder Journaldateien lassen sich unvollständige Transaktionen identifizieren und wiederherstellen.
- AE0 – Betrieb mit Unterbrechungen, wobei die Verfügbarkeit der Daten nicht wesentlich ist. Der Benutzer kann nicht weiterarbeiten, das System fährt unkontrolliert herunter. Daten

können verloren gehen oder verfälscht werden.

Verifikation – Verification

Die Verifikation prüft, ob das Ergebnis einer Lebenszyklusphase die zu Beginn der Phase gestellten Anforderungen erfüllt. Dies beinhaltet die Überprüfung der Sicherheitsanforderungen.

Verschlüsselung – encoding

Verschlüsselung soll Nachrichten und Daten vor unberechtigter Kenntnisnahme und Manipulation schützen. Die zu schützenden Informationen werden nach einem festgelegten Verfahren (Algorithmus) und unter Einsatz eines „Schlüssels“ oder Codes in einen Geheimtext (Chiffre) übersetzt. Ohne den Schlüssel darf es Unbefugten nicht möglich sein, den Geheimtext zu entschlüsseln. Zur Verschlüsselung von Druckdaten existiert das Internet Printing Protocol (IPP), Version 1.1. Dies ist in den RFCs 2910, Internet Printing Protocol/1.1: Encoding and Transport, RFC 2911, Internet Printing Protocol/1.1: Model and Semantics, und RFC 3196, Internet Printing Protocol/1.1: Implementor's Guide, beschrieben. Die Transportschicht basiert auf http 1.1 und kann http-Erweiterungen wie SSL und TLS verwenden.

Verteilter DoS-Angriff – Distributed Denial of Service (DDoS) Attack

Großflächiger Angriff, bei dem eine Vielzahl von Systemen ein Zielsystem oder –Netzwerk lahm legen.

Vertrag auf Gegenseitigkeit – Reciprocal Agreement

Bei einem Vertrag auf Gegenseitigkeit vereinbaren zwei oder mehrere Parteien, z. B. Unternehmen, Unternehmenstöchter oder Organisationseinheiten, die prinzipiell gleichartige Schutzobjekte nutzen, dass sie z. B. im Katastrophenfall Schutzobjekte des Vertragspartners nutzen können, um dort den Notbetrieb durchzuführen.

Vertraulichkeit – Confidentiality

Eigenschaft eines Objekts bzw. einer Information, nur Befugten (Personen, Prozessen oder Ressourcen) bekannt bzw. zugänglich zu sein.

Verwundbarkeit – Vulnerability

Eigenschaft eines Objektes, z. B. eines Informationssystems oder eines Rechenzentrums, gegenüber bestimmten Ereignissen, z. B. Stromausfall oder Hacker-Angriffen, ungeschützt zu sein.

Vier-Augen-Prinzip

Das Vier-Augen-Prinzip ist eine Methode der gegenseitigen Kontrolle und Verantwortung durch Hinzuziehung einer zweiten Person.

Virtuelles LAN (VLAN) – Virtual LAN

Virtuelle LANs (VLANs) sind logische Netzsegmente, die der Bildung von Sicherheitszonen mit unterschiedlichem Sicherheitsniveau dienen. Sie entstehen durch die Aufteilung eines physikalischen Netzes in logische Netzsegmente, die durch entsprechend konfigurierte Switches gebildet werden.

Virtuelles privates Netz (VPN) – Virtual Private Network (VPN)

Ein virtuelles privates Netz stellt eine gesicherte Verbindung über ein öffentliches Netz dar.

Virus – virus

s. Computervirus

Vishing

Vishing ist ein Kunstwort für „Voice over IP Phishing“. Hierbei nutzen Angreifer die niedrigen Kosten und die weltweite Verfügbarkeit der Internettelefonie für meist automatisierte Anrufe. Ein Dialer ruft eine Vielzahl von VoIP-Adressen an. Im Telefonat täuscht eine Stimme von Band vor, der Anruf käme von einer vertrauenswürdigen Instanz, z. B. einem Finanzinstitut. Die Stimme veranlasst das potenzielle Opfer, vertrauliche Daten, insbesondere Kreditkartennummer, Kontonummer, PIN und TAN preiszugeben, so dass der Angreifer an die Finanzen des Opfers gelangen kann. Ebenfalls abgefragt werden können Geburtstag, Sozialversicherungsnummer und Passnummer, um Identitätsdiebstahl begehen zu können. Die Auswertung der Anrufe kann auf Seiten des Anrufers ebenfalls automatisiert erfolgen. Hierzu wandelt ein System entweder die per Tastatur eingegebenen Ziffern um, indem es die Töne der Ziffern in digitale Zeichen umsetzt oder es verwendet die Spracherkennung. Anstelle des automatisierten Anrufs kann der Angreifer zuvor eine E-Mail oder eine SMS einer scheinbar vertrauenswürdigen Instanz an das Opfer schicken, die es dazu veranlasst, die vom Angreifer vorgegebene Telefonnummer anzurufen.

VIVA

Abkürzung für Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität

Voice over Internet Protocol (VoIP)

Voice over IP ermöglicht die Sprachkommunikation über das Internet und treibt die Konvergenz von Sprache und Daten vor-

an. Dadurch ist z. B. nur noch eine Verkabelung erforderlich. Wie immer bei der Nutzung des Internets sind hierbei Sicherheitsaspekte zu berücksichtigen. Bedrohungen bestehen in Form von Ausfällen, Störungen, Verzögerungen und Angriffen u. a. durch Viren und Würmer, SpIT (Spam over Internet Telephony), IP-Spoofing, Man-in-the-Middle-Attacken und durch Abhören mit derzeit bereits verfügbaren Tools, z. B. mit VoMIT (Voice over Misconfigured Internet Telephones).

Die vielfältigen Bedrohungen verlangen angemessene Sicherheitsmaßnahmen, z. B. in Form ausfallgeschützter Stromversorgung und Ausweichmöglichkeiten bei Ausfällen oder Störungen, einer für VoIP geeigneten Firewall, Intrusion Detection and Prevention System, Virenschutz, Content Filter, Verschlüsselung und VPN. Eine anforderungsgerechte Quality of Service (QoS) erfordert u. a. die Vermeidung von Übertragungsverzögerungen und Paketverlusten sowie eine garantierte ausreichende Bandbreite, die durch das Bandbreitenmanagement sicherzustellen ist. Die im Februar 2005 gestartete VoIP Security Alliance (VOIPSA) beschäftigt sich mit Sicherheitsaspekten von VoIP.

W

Wassermeldeanlage (WMA)

Wassermeldeanlagen gehören zu den Gefahrenmeldeanlagen. Sie dienen dazu, Flächen, Räume, Rohrleitungen und andere Einrichtungen auf den Austritt leitender Flüssigkeiten, wie z. B. Wasser, zu überwachen.

Webcrawler

Webcrawler durchsuchen das World Wide Web und analysieren Webseiten. Suchmaschinen nutzen diese Programme.

Weitverkehrsnetz – Wide Area Network (WAN)

Ein Weitverkehrsnetz ist ein nicht lokales Verbindungsnetz, das einen größeren geographischen Bereich abdeckt und von einem eigenständigen Betreiber angeboten wird.

Werbe-E-Mail – Spam-Mail

Unerwünschte Werbe-E-Mails werden als Spam-Mails bezeichnet, die gleichzeitige Versendung an eine Vielzahl von Empfängern als „Spamming“, der Absender als „Spammer“.

Werbesoftware – Adware

Werbesoftware (Adware) sammelt auf dem betroffenen Computer Informationen für Werbezwecke. Auf Basis dieser Informationen können Anbieter festlegen, welche Werbe-Popup-Fenster

auf dem Computer eingeblendet werden und welche Werbungen der Computernutzer angezeigt bekommt, wenn er bestimmte Webseiten besucht.

Wiederanlauf – Recovery

Wiederanlauf bezeichnet das Verfahren zum Start aller erforderlichen Prozesse und Systemkomponenten nach Systemabstürzen bzw. –ausfällen, um entweder den regulären Betrieb wieder herzustellen oder den Notbetrieb anzufahren.

Wiederherstellung – Restoration

Wiederherstellung bezeichnet das Verfahren zur Instandsetzung ausgefallener Schutzobjekte, z. B. Gebäude, Systeme oder Komponenten, durch Reparatur oder Ersatzbeschaffung.

X

XML

Die eXtensible Markup Language ist eine einfache und flexible Auszeichnungssprache zur Darstellung von Daten im Textformat, die aus SGML abgeleitet wurde. Sie gewinnt nicht zuletzt auch beim Datenaustausch z. B. über das Internet, zunehmend an Bedeutung.

Z

Zentrale Rechtesteuerung und –verwaltung – Single Point of Security Control and Administration (SPSCA)

Die zentrale Rechtesteuerung und –verwaltung umfasst die Eingabe, Pflege, Sperrung, Freigabe und Löschung von Rechten und die darauf aufbauende Steuerung von Berechtigungsanfragen.

Zentrale Rechteverwaltung – Single Point of Security Administration (SPSA)

Zentrale Rechteverwaltung ist die Stelle, an der die Rechte für z. B. ITK-Systeme verwaltet, d. h. administriert werden.

Zero-Day-Attacke

Eine Zero-Day-Attacke ist ein Angriff, der in dieser spezifischen Form erstmalig ist. Sie nutzt umgehend, also quasi am gleichen Tag (zero day), eine gerade erst bekannt gewordene Sicherheitslücke aus, noch bevor die Sicherheitslücke durch Patches geschlossen wurde oder verbreitet einen neuen Virus noch bevor entsprechende Signaturen für die Computer-Antiviren-Software verfügbar sind.

Zufahrtsschutz

Der Zufahrtsschutz dient dazu, die Zufahrt zum Grundstück sowie in das Gebäude abzusichern, indem nur berechtigten Personen und Fahrzeugen Zufahrt gewährt wird.

Zugangsschutz

Der Zugangsschutz dient dazu, den Zugang zu Informationssystemen und den unternehmenseigenen Netzen abzusichern, indem sich Benutzer und Systeme identifizieren und authentisieren müssen. Dies erfolgt oftmals durch die Benutzerkennung (UserId) und das Passwort. Darüber hinaus sollte der Zugang zum unternehmenseigenen Netz zusätzlich durch Firewalls sowie bedarfsorientiert durch Intrusion-Detection-, -Response- und -Prevention-Systeme abgesichert werden.

Zugriffskontrollliste – Access Control List

In der Zugriffskontrollliste führt das Betriebssystem die Liste mit Zugriffsberechtigungen auf Objekte.

Zugriffsschutz – Access Control

Der Zugriffsschutz dient dazu, den Zugriff auf Objekte, wie z. B. Programme und Daten abzusichern, indem nur berechtigten Subjekten, wie z. B. Personen oder Anwendungen, und diesen nur mit bestimmten Rechten, wie z. B. lesen oder schreiben, Zugriff auf diese Objekte gewährt wird.

Zutrittsschutz

Der Zutrittsschutz dient dazu, den Zutritt zu Gebäuden und Räumlichkeiten abzusichern, indem nur berechtigten Personen Zutritt gewährt wird.

Zuverlässigkeit – reliability

Zuverlässigkeit beschreibt die Eigenschaft eines Prozesses, einer Ressource, eines Produktes oder einer Dienstleistung innerhalb eines betrachteten Zeitraums die an ihn/sie gestellten Anforderungen zu erfüllen. Kenngrößen sind die Lebensdauer und die Ausfallwahrscheinlichkeit.

Sachwortverzeichnis

3

3D-Face	294
3D-Pyramidenmodell	10
3D-Sicherheitspyramide	10

4

4Vs	65, 137

A

AAA	454
ABAS	288
Abfahrtskontrolle	215, 242
Abgabenordnung	103
Abgangskontrolle	215, 242
ABIS	288
Abnahmehandbuch	358
Abnahmeprozess	358
Absendekontrolle	215, 241
Abstand	316
Abweichungsanalyse	374
AC	272
Access Control List	425
Accessmanagement	230
ACL	425
Adware	472
AEC	469
AES	237
AGG	292
Agreement	
- Reciprocal	470
- Service Level	458
AktG	405
Alarm	425

Alarmierung	216, 243
Alert	425
Alignment	44
- Business ICT	44
- Business-Safety-Security	44
- Business-Safety-Security-Continuity-Risk	39, 44
- Business-Security	44
Änderungsmanagement	185
Anforderungsarchitektur ...	132
Anforderungsprofil	261
Angriffssicherheit	56, 131, 153
Anhängsel	425
Anomalie	425
- Erkennung	281
- statistische	281
Anomalieerkennung	425
Anomaly	425
Anomaly Detection	425
ANSI	425
Antrags- und	
Genehmigungsverfahren	
- Zugang, Workflow	325
Anwendungsschicht-Gateway	425
AO	405
API	443
Appliance	260, 275, 425
Application Level Gateway	278, 425
Application Response	
Measurement	425
Application Vulnerability	
Description Language	256
architecture	
- requirements	132
Architektur	
- Anforderungs-	132
- Bedrohungen	135, 170

- Schäden..... 170
- Schwachstellen..... 171
- Architekturmanagement ... 246
- Archivierung
 - Konzept..... 354
 - Strategie 267
- ARM 425
- asset 369
- Attachment 425
- Attacke
 - Before-Zero-Day 287
 - Brute-Force 427
 - Denial-of-Authentication 293
 - Replay 293
 - Zero-Day..... 287
- auditing 250, 257
- Aufbewahrungsfrist 104
- Ausfall
 - Dienstleister 3
 - Mobilfunknetz 3
 - Strom..... 2
- Ausfalldauer..... 140
- Ausfallzeit..... 426
- Auslagerung 197
- Auslagerungsstrategie 207
- Auslöser 426
- Außerbetriebnahme 361
- authentication on device... 293, 294
- Authentifizierung 426
- Authentifizierungssystem
 - biometrisch..... 288
- Authentisierung..... 426
- Authentisierung durch
 - Besitz..... 222
 - Besitz und Merkmal.... 222, 223
 - Merkmal 222
 - Merkmal und Wissen.. 222, 223
 - Verhalten 222, 223
 - Wissen..... 222

- Wissen und Besitz. 222, 223
- authority 250
- Autorisierung 426
- Availability..... 469
- Availability Environment
 - Classification..... 469
- AVDL..... 256, 416
- awareness..... 41, 264
- AWI..... 440
- AWV 409

B

- Backup 276
- Balanced Scorecard 377
- Bandbibliothek 276
- BankG 406
- BankV..... 406
- Basel II..... 9, 106, 409
- Bastion-Host..... 280, 426
 - entmilitarisierte Zone... 280
 - kaskadiert..... 280
 - Secure-Server-Network 280
- BCM 58, 445
 - holistic 60, 445
 - Pyramide 61, 445
- BCM pyramid 61
- BCMS 42
- BCP..... 42, 58
- BDSG..... 106, 405
- Bedrohung..... 132, 426
 - Anwendungsmängel 6
 - Computerattacken 4
 - Computerkriminalität 3
 - Computerviren 4
 - Datendiebstahl 5
 - Datenverlust 5
 - Epidemien..... 3
 - Feuer 3
 - Hochwasser 3
 - Pharming..... 5
 - Phishing..... 5

- prinzipiell 132
- Software-Änderung 6
- Update 6
- Bedrohungsanalyse 170
- Bedrohungsarchitektur 135, 170
- Bedrohungslandkarte 134
- Before-Zero-Day-Attacke .. 287
- Begleitprozess
 - Änderungsmanagement 185
 - Architekturmanagement 246
 - Datenschutzmanagement 166
 - Ereignismanagement ... 178
 - Finanzmanagement 176
 - Innovationsmanagement 259
 - Kapazitätsmanagement 190
 - Konfigurationsmanage-
ment..... 188
 - Konformitätsmanagement 165
 - Kontinuitätsmanagement 193
 - Leistungsmanagement 172
 - Lizenzmanagement..... 190
 - Performancemanagement 190
 - Personalmanagement .. 261
 - Problemmanagement... 184
 - Projektmanagement 177
 - Qualitätsmanagement . 177
 - Releasemanagement 188
 - Risikomanagement 168
 - Securitymanagement ... 211
 - Service Level Management 172
 - Wartungsmanagement 192
- Begleitprozesse 155
- Begrenzungsrouter 279
- BEL 44
- Benchmark
 - Safety-Security 380
- BEntA..... 44
- Benutzerfreundlichkeit..... 261
- Benutzerkonto 326
 - gesperrtes..... 328
- Benutzerservice 178
- Berechtigungskubus ... 217, 426
- Berechtigungswürfel .. 217, 426
- Berichtswesen
 - Anforderungen 374
 - IT-Sicherheit 374, 377
 - Safety 374
 - Safety/Security 374
 - Security..... 374
- Betrieb..... 360
 - regulär 197
 - Rückkehr 194
- Betriebseinflussanalyse 110, 426
- Betriebsführungshandbuch 353
- Betriebssicherheit .. 55, 131, 153
- Beweissicherung..... 243
- BGB 101
- BIA 58, 108, 428, 437
- biometric hacking..... 292
- biometric system 288
- Biometrische Verfahren
 - Akzeptanz..... 294
 - monomodale..... 294
 - multimodale 294
 - multispektrale 294
- Biometrisches System 288
 - capture..... 291
 - decide 291
 - enrolment..... 290
 - extract..... 291
 - match 291
 - template 290
 - Registrierung..... 290
- blacklist..... 285
- Blacklist Model 452
- BMA 199, 427

BOSS 371
 Böswillige Software 427
 Botnet 427
 Brandmeldeanlage..... 199, 427
 Brute-Force-Attacke 427
 Brutto-Risiko 63
 BS 15000 414
 BS 25999-1 69, 96
 BS 25999-1, 2006 ... 39, 410, 445,
 459
 BS 25999-2 42, 96, 410
 BSA 44
 BSI 23, 428
 - 100er Reihe 36
 - Bausteinkatalog 34
 - IT-Sicherheitskonzeption
 34
 - IT-Sicherheitsprozess 33
 - Standard 100-1 36, 410
 - Standard 100-2 36, 410
 - Standard 100-3 36, 410
 BSSCRA 39, 44
 Buchführung
 - ordnungsmäßige 103
 Buffer-Overflow.. 245, 354, 355
 Bunch of Disks
 - JBOD 274
 - MBOD 274
 - SBOD 274
 Bundesdatenschutzgesetz . 428
 BuPROPSeLiA 44
 Business Continuity
 - Joint Forum 418, 445
 - Management 324
 Business Continuity
 Management 58, 445
 - BS 25999-1, 2006 410
 - BS 25999-2 410
 - ganzheitlich 60, 445
 - holistic 60, 445
 Business Continuity Plan.... 58,
 195
 Business Continuity Planning

- FFIEC 408, 445
 Business Enterprise
 Alignment 44
 Business Enterprise Linkage 44
 Business Impact Analysis.... 58,
 108, 428, 437, 457
 BuSSeCoRA 44
 BWG 406

C

CAdES 256
 CAP 256, 416, 429
 capability 384
 Capability Maturity Model
 - Systems Security
 Engineering 384
 CBCO 298
 CCO 297, 394, 429
 CD 440
 CEO 101
 CERT® 429
 Certified Information Security
 Auditor™ 428
 Certified Information Security
 Manager™ 428
 CFO 101
 CFR
 - 21 CFR Part 11 408
 Challenge 451
 Challenge Handshake
 Authentication Protocol . 428
 Challenge-Response-
 Verfahren 226, 429
 Change History 186
 Change Management 185
 Change Request 185
 CHAP 428, 451, 454
 Check-out-check-in-Prozedur
 186
 Chief Business Continuity
 Officer 298

- Chief Compliance Officer. 297, 429
- Chief ICT Continuity Officer 297
- Chief ICT Security Officer. 297
- Chiffrierung..... 236
- Chipkarte 429
- Choreografie..... 247
- CIA 429
- CIA² 429
- CICO..... 297
- CIFS 273
- CIM..... 276
- circle of trust..... 229
- Circuit-Level-Gateway278, 429
- CISA™ 428
- CISM™..... 428
- CISO 297, 394
- Clear Desk Policy..... 453
- Closed-Shop-Betrieb 148
- Cluster-System..... 201
- CMDB..... 183, 350
- CMM® 411
- CMMI® 38, 411
- COBIT® 37, 69, 411
 - Domänen 38
 - Kontrollziele..... 39
 - Prozessmodell..... 38
 - Rahmenwerk..... 38
- COBIT®..... 95
- Code-Injection 245
- Code-Signierung..... 256
- Code-Signing Profile 416
- COLD 430
- Command Injection..... 354
- Commodity 231
- Common Alerting Protocol256
- Common Criteria, 2006..... 52
- Compliance 165, 429, 444
 - IT..... 441, 444
 - ITK..... 441, 444
- Computer Emergency Response Team 429
- Computer Security Emergency Team 182
- Computer Security Incident Response Team182, 298, 360, 430
- Computerattacken 4
- Computerkriminalität 3
- Computerviren 4
- Computervirens Scanner 286
- Computervirus 430
- Configuration Item 350
- Configuration Management Database 350
- Content-Security-System ..285, 431
- Continuity 131, 153
 - Incident Response..... 181
- Continuity Management 193
 - Business.....58
 - IT Service.....418
- control.....446
 - objective 446
- Controls
 - Application - 102
 - Compliance.....166
 - Continuity 210
 - General IT - 102
 - Maturity 389
 - Policy 85
 - Privacy.....168
- COPPA 408
- CR.....185
- Cracker 431
- criticality 446
- CRO.....394
- Cross-Site-Scripting 354, 431
- CSIRT 182, 298, 360, 430
- CSO 394
- CSPP-OS 411
- CSS 431
- CTI.....183

D

DAC.....	432
Daktyloskopie	291
DAS.....	272, 273, 432
Data Striping	271
Dateiviren	286
Datendieb.....	451
Datendiebstahl	5
Datenlöschung	5
Datenschutzbeauftragter ...	298
Datenschutzmanagement ..	166
Datensicherung.....	197
- Archive	206
- Aufbewahrung.....	317
- Auslagerungsverfahren	207
- Aussonderungsfrist.....	317
- Container	411
- differenziell	203
- Dokumentationsvorlage	342
- Generationen.....	204
- Generationenprinzip....	317
- inkrementell	203
- komplett.....	202
- Konzept.....	354
- Medien	317
- Methoden	203, 204
- Namenskonventionen..	317
- Plan.....	317
- Prozess	154
- Räume	411
- Ressourcen	154
- Richtlinie.....	317
- Schränke	411
- selektiv	204
- Sicherheitszeitpunkt	205
- Strategie	266
- Verantwortlichkeit	154
- Verfahren.....	317
- zeitgleich.....	205
- zeitnah.....	205
- zeitversetzt	205

Datenträgerarchiv	200
Datenträgerkataster	317
Datenträgervernichtung.....	241
- chemisch.....	241
- mechanisch	241
- thermisch.....	241
Datenverlust.....	5
- maximal tolerierbarer...	455
- Recovery Point Objective	455
Datenvernichtung	240
DDoS.....	470
De-Duplizierung	276
De-Gausser.....	240
Demilitarisierte Zone.....	431
Demilitarized Zone	434
Denial of Service.....	432
Deny-All-Prinzip.....	147
DES.....	237
Detaillierter Risikodreiklang	63
nach Dr.-Ing. Müller	63
DHCP.....	433
Dienstleistungssicherheit	77
- lebenszyklusimmanent	77
Digital Rights Management	431
Digital Signature Services ..	255
digitale Signatur	256
Digitales Rechtemanagement	431
Digitales Wasserzeichen.....	432
DIN 16557-4	411
DIN 16560-15	411
DIN 32757-1	411
DIN EN 12251	411
DIN EN 50126.....	411
DIN EN 62040-3.....	411
DIN EN ISO 9001	107, 411
DIN ISO 9735-9.....	411
Direct Attached Storage	272, 273, 432
DIS.....	440
Disaster-Recovery-Plan	195

Discretionary Access Control	432	eGrid	258
Distanzanforderung	317	EICAR	433
- Müllersche	317	Einbruchmeldeanlage	214, 433
Distanzprinzip	317	Eindringling	245
- Müllersches	317	Einmal-Passwort	225
DLL Injection	245	Ein-Schlüssel-Verfahren	237
DLM	432	Eintrittswahrscheinlichkeit	433
DMZ	434	Electronic Data Interchange	433
DNS	432	Electronic PostMark Profile	417
Dokumentenlebenszyklusmanagement	432	EMA	214, 433, 434
domain	384	Emergency Data Exchange Language	257
Domain Name Services	432	EN 1047-1	411
DoS	432	EN 1047-2	411
downtime	426	Engineering	
DPPA	408	- Safety and Security	47
DRM	431	- Safety, Security and Continuity	47
Dronen	261	enrolment	290
Druckjob	260	Enterprise Grid Alliance	258
- Ausgabe	260	Entfernung	
DS	272	- Standorte	316
DSG	106, 406	entmilitarisierte Zone	280, 434
DSG 2000	106, 406	ePass	291
DSS	255, 416	Epidemien	3
DTDS	272, 317	Ereignis	
DTDS+	272, 317	- sicherheitsrelevant	243
Dynamic Host Configuration Protocol	433	Ereignismanagement	178
		Erhaltungssatz	152
E		Escrow-Agentur	175, 358
EBK-RS 95/1	406	ESSCMS	20
EBK-RS 98/1	407	Etagenverteiler	200
EBK-RS 99/2	407	eTAN	464
ebXML	413, 433, 466	eTAN plus	464
EDI	433	Ethernet	273
EDIFACT	411, 433	- Gigabit	273
EDXL-DE	257	Europäische Richtlinien	407
EEPROM	267	EuroSOX	102
EFF	246	Exploit	434
EGA	258		

F

Fabrics	274
FAIT 1.....	104
FAIT 2.....	104
FAIT 3.....	104
Falsch negativ.....	434
Falsch positiv.....	434
Falschakzeptanzrate.....	290
Falschrückweisungsrate	290
False Acceptance Rate223, 239, 290, 434	
False negative.....	434
False positive.....	434
False Rejection Rate ... 223, 239, 290, 434	
FAR.....	223, 239, 290, 434
FC.....	435
FC-AL.....	274
FCIP	276
FDIC	
- Managing Multiple Service Providers.....	408
- Selecting a Service Provider	408
FDIS	440
Federal Data Protection Act	428
fehlertoleranter Rechner	201
FERPA	408
Festkörpersensor.....	291
FFIEC	
- Business Continuity Planning.....	408, 445
- Outsourcing	408
- Supervision of Technology Service Providers	408
Fibre Channel	435
Fibre-Channel-Arbitrated- Loop.....	274
FIDIS.....	232
Financial Transaction Services	435

Finanzmanagement	176
Fingerabdruck	291
Fingerabdrucknehmen	435
- aktiv	435
- passiv	435
Fingerabdrucksensor	291
- drucksensitiv	291
- Festkörper	291
- hochfrequent.....	291
- optisch	291
- thermisch.....	291
- Ultraschall nutzend	291
Fingerprint Scanner	291
Fingerprinting.....	435
FinTS	412, 435, 439
FinTS HBCI	435
FinTS PIN/TAN	435
Firewall.....	276, 436
- Appliance	279
- Application Level Gateway.....	278
- Bastion-Host	280
- Begrenzungsrouter	279
- Circuit-Level-Gateway	278
- Dual-Home	280
- Multi-Home	280
- Paketfilter	278
FIRST.....	436
FISMA.....	408
Flächensensor	291
Flash-EEPROM.....	267
FoIA.....	407
forensische Codes.....	246
forensische Computeranalyse	244
forensische Informatik	244, 436
forensische Psychologie	262
forensischer Informatiker....	245
forensischer Sachverständiger	244
FRR.....	223, 239, 290, 434
Funk-LAN	436
Funktionstrennung	146, 437

G

- GAMP 107, 412
- GCE 259
- GDPdU 409
- Gebäude 199
- GeBüV 407
- Gefahrenmeldeanlage 437
- Geldfälscher 246
- Geldwäschereigesetz 407
- Geldwäschereiverordnung 407
- Generationenprinzip 197
- Generische
 - Sicherheitskonzepte 74
- GERM 107, 412, 454
- Geschäftsbücherverordnung 407
- Geschäftseinflussanalyse 58, 108, 437
- Geschäftskontinuität 58
- Geschäftskritikalität 98
- Gesetze
 - Österreich 406
 - United Kingdom 407
 - USA 408
- GGF 258
- GLBA 408
- Global Grid Forum 258
- GLP 107
- GMA 437
- GmbHG 405
- GMP 107
- GoB 409
- GoBS 409
- GoDV 409
- GoS 409
- Governance
 - Information Security 23, 95
 - IT 441
 - ITK 441
- Grenzzenarien 91
- Grid
 - EGA 258
 - GGF 258
 - OGFSM 258
- Grid Computing Environment 259
- Grid-Computing 257
- Grids 437
- Grundsätze
 - GDPdU 103
 - GoB 103
 - GoBS 103
 - GoDV 103
- GSHB
 - IT 416
- GwG 405, 407
- GwV EBK 407

H

- Hacker 438
- Handbuch
 - Abnahme 358
 - Generierung 358
 - Notfall- und Katastrophenvorsorge 320
- Handelsgesetzbuch 103
- Harvester 438
- Hash-functions
 - ISO/IEC 10118 412
- Hashwert 255
- Haus zur Sicherheit 120
- Hazard and Operability Analysis 438
- HAZOP 368, 438
- HBCI 412, 439
- hBCM 60, 445
- HGB 405
- HIDS 282
- hoax 434
- Hochwasser 3
- Home Banking Computer
 - Interface 439
- honeyd 283

Honeynet	283	IdM.....	230
Honeypot	283	IDS.....	282, 441
- Sticky.....	284	IDW	439
Honeytoken.....	284	- PS 330.....	409
honeytrap.....	283	IDW	
Honignetz	283	- PS 880.....	409
- virtuell.....	284	- RS FAIT 1	409
Honigtöpfchen	283	- RS FAIT 2	409
HoSSC	120	- RS FAIT 3	409
Host	282	IEC.....	439
hot fixes.....	186	IEC 62040-3.....	411
hot pluggable	201	IETF	440
hot space	271	iFCP.....	276
hot spare	271	IKS.....	103
hot swap.....	271	IKT.....	25
hot swappable.....	201	ILM.....	439
House of Safety, Security and Continuity.....	120	IMAP.....	440
		IMAPs	440
<i>I</i>		IMP	41
IAM.....	231	Impact Analysis	
IAS	261	- Business.....	108
ICT	25	- Operational	110
ICTSKRMS.....	394	impact architecture	
ICTSMS	394	- business	170
IDEA™.....	237	- resource	170
Identifikationssystem		In-Band-Virtualisierung	275
- biometrisch.....	288	Incident Detection	
Identitätsmanagement 230, 260		- Security/Continuity	181
- föderiert	229	Incident Response	181
- Liberty Alliance	229	Incident-Management-Plan	41
Identitäts-Provider	229	indizierte TAN.....	464
Identity		Information Security	
- Life Cycle.....	230	Governance	23, 95
- maintaining	230	Information Security Incident Management	360
- Management	230	Informations- und Tele- kommunikationssysteme	
- provisioning.....	230	- Vorgaben.....	200
- terminating.....	230	Informationslebenszyklus- management	439
Identity Management		Informationssicherheits- managementsystem	21
- Federated.....	229		
Identity-Provider	254		

-
- Informationssicherheitspolitik
 - nach ISO/IEC 17799 52
 - nach ISO/IEC 27001 53
 - nach ISO/IEC 27002 52
 - InfoSiG 406
 - InfoSiV 406
 - Infrastruktur 295
 - Gebäude 199
 - Räumlichkeiten 200
 - ingenieurmäßige Sicherheit 47, 439
 - Innovationsmanagement... 259
 - Integrität 468
 - persönliche 262
 - Integritätstest 262
 - Interdependenzbaum 322
 - Interdependenznetz 322
 - Interdependenzplan 322
 - International Engineering Consortium 439
 - International Organization for Standardization 440
 - Internes Kontrollsystem 102, 103
 - Internet
 - iFCP 276
 - iSCSI 276
 - Internet Engineering Task Force 440
 - Internet Message Access Protocol 440
 - Internet Printing Protocol.. 470
 - Internet-Analyse-System ... 261
 - Internet-Verfügbarkeits-System 261
 - Inter-Network communication
 - ISO/IEC 18028-3 414
 - Intruder 245
 - Intrusion
 - Detection 282
 - Prevention 282
 - Protection 282
 - Response 282
 - Intrusion-Detection-System 281, 441
 - hostbasiert 282
 - netzbasiert 281
 - Intrusion-Signature 281
 - Intrusion-Signature-Detection 449
 - IP-Adresse 432
 - IP-Masquerading 441
 - IPP 470
 - IPS 282
 - IPsec 441
 - IP-Spoofing 441
 - IP-Stack 435
 - IRS 282
 - ISACA® 37
 - iSCSI 276
 - Isi-BSC 365
 - ISiPyr 441
 - ISKRMS 394
 - ISMS 21, 28, 36, 394
 - Politik 53
 - ISMS-T 418
 - ISO 440
 - ISO 15489 454
 - ISO 15489-1 413
 - ISO 15489-2, TR 413
 - ISO 20000 69
 - ISO TS 15000 413
 - ISO/DIS 27799 415
 - ISO/IEC 10118-1 412
 - ISO/IEC 10118-2 412
 - ISO/IEC 10118-3 412
 - ISO/IEC 10118-4 412
 - ISO/IEC 13335 24, 107, 412
 - ISO/IEC 13335-1 68, 96
 - ISO/IEC 13335-2 26
 - ISO/IEC 13335-5 26
 - ISO/IEC 13888 412
 - ISO/IEC 15408 69, 413
 - ISO/IEC 15443, TR 413
 - ISO/IEC 15446, TR 413
 - ISO/IEC 15504, TR 413

ISO/IEC 15946	413	- Firewall Guidelines and Policy.....	416
ISO/IEC 17799 .. 26, 68, 96, 107, 414		- IDPS	416
ISO/IEC 18028	414	- Product Selection Guide	416
ISO/IEC 18028-1	26, 414	- Self-Assessment.....	370
ISO/IEC 18028-2	414	- Self-Assessment Guide.....	416
ISO/IEC 18028-3	414	- Training Requirements	416
ISO/IEC 18028-4	414	IT Service Lifecycle	163
ISO/IEC 18028-5	414	IT Service Management	
ISO/IEC 20000	96, 107	- ISO/IEC 20000-1	414
ISO/IEC 20000-1	414	- ISO/IEC 20000-2	414
ISO/IEC 20000-2	414	iTAN	464
ISO/IEC 21000-5	414	IT-Betrieb.....	360
ISO/IEC 21827	414	IT-Compliance	441, 444
ISO/IEC 24759, FCD	414	ITC-Securitymanagement	
ISO/IEC 24760, NP	414	- ISO/IEC 13335.....	412
ISO/IEC 24761, FCD	415	ITGI®	37
ISO/IEC 24762, FCD	415	IT-Governance	441
ISO/IEC 24764, NP	415	IT-Grundschutzhandbuch ..32,	
ISO/IEC 27000, FCD	415	69, 96, 416	
ISO/IEC 27000-Reihe	30	IT-Grundschutzkataloge	32
ISO/IEC 27001	28, 68, 96	IT-GSHB	32, 416
ISO/IEC 27002 ... 26, 68, 96, 415		IT-GSK	416
ISO/IEC 27003	415	ITIL® 31, 69, 96, 107, 162, 416	
ISO/IEC 27004, FCD	415	- Service Design	164
ISO/IEC 27005, FCD	415	- Service Improvement ...	164
ISO/IEC 27006	415	- Service Lifecycle.....	163
ISO/IEC 27051	415	- Service Operation.....	164
ISO/IEC DIS 29361	415	- Service Strategy	164
ISO/IEC DIS 29362	415	- Service Transition	164
ISO/IEC DIS 29363	415	- Version 3	163
ISO/IEC DIS 29382	416	ITK.....	25, 442
ISO/IEC PRF TR 24731	414	ITK-Betrieb.....	360
ISO/IEC TR 13335-3	26	ITK-Lebenszyklus	347
ISO/IEC TR 13335-4	26	ITK-Schutzbedarfsanalyse .	110
ISO/IEC TR 15947	414	ITK-Sicherheitsmanagement	23
ISO/IEC TR 18044	414	ITK-Sicherheitspolitik.....	51
ISP	454	ITKSiPyr	442
IT Governance Institute® 23, 95		ITKSKRMS	394
IT Security		ITK-Systemsicherheit	
- Assessment Framework	385, 416	- lebenszyklusimmanent ...	77
- Engineering Principles. 416		IT-Lebenszyklus	347

ITSCM	442
ITSEC.....	416
IT-Security	
- ISO/IEC TR 18044	414
IT-Securitymanagement	
- ISO/DIS 27799	415
- ISO/IEC 13335	24
- ISO/IEC 13888-1,2,3	413
- ISO/IEC 14888-1,2,3	413
- ISO/IEC 15443-1,2,3, TR413	
- ISO/IEC 15446, TR.....	413
- ISO/IEC 15946	413
- ISO/IEC 17799	414
- ISO/IEC 17799, 2005	26
- ISO/IEC 27000, FCD	415
- ISO/IEC 27000-Reihe.....	30
- ISO/IEC 27001	28
- ISO/IEC 27002	415
- ISO/IEC 27002, 2005	26
- ISO/IEC 27003	415
- ISO/IEC 27004, FCD	415
- ISO/IEC 27006	415
- ISO/IEC 27051	415
- IT-GSHB	416
IT-Services	163
IT-Sicherheits-BSC.....	365
IT-Sicherheitsprozess	33
ITU.....	415
ITU-T	442
IuK.....	25
IuKDG	405

J

JAAS.....	443
Java™ Authentication and Authorization Service	443
Java™ Cryptographic Extension	443
Java™ Secure Socket Extension	443
JBOD.....	274

JCE.....	443
Joint Forum	
- Business Continuity.....	418, 445
- Outsourcing	418
JSSE	443

K

KAGG	406
kanonisch	255
Kapazitätsmanagement.....	190
KDC	227
Kennzahl	321
Kerberos™	227, 443
Kernprozess	154, 156
Key Distribution Center.....	227
Key Performance Indicator	378
Key-Logger	241, 444
Klassen-Maßnahmen-Matrix	126
KMM.....	126
KMU	
- Sicherheitsmanagement.	17
KNOPPIX.....	372
Kommunales Netz	444
Konfigurationscluster	189
Konfigurationsdatenbank .	189, 350
Konfigurationselement.....	188, 350
Konfigurationsmanagement	188, 189
Konfigurationsmanager	350
Konformität.....	165, 444
Konformitätsmanagement.	165
Konsolidierung	
- Dataware.....	150
- Hardware	150
- Interface.....	150
- Knowledgeware.....	150
- Middleware	150

- Orgware.....	150
- Processware.....	150
- Prozess	150
- Schnittstellen	150
- Software.....	150
- Technologie	150
- Wissen.....	151
Kontinuitätsmanagement. 193,	195, 445
Kontinuitätsmanagement-	
pyramide.....	91
Kontinuitätspolitik	73
Kontinuitätspyramide.....	445
KonTraG	168, 406
Kontrollaktivität	446
Kontrollelement	446
Kontrollen	
- Datenschutzmanagement	
.....	168
- Konformitätsmanagement	
.....	166
- Kontinuitätsmanagement	
.....	210
- Politik	85
- Reifegrad	389
Kontrollziel	446
Konversation	247
Korrekturmaßnahmen	374
Kosten	
- Sicherheitsverletzungen ..	4
Kosten-Nutzen-Aspekte	88
KPI	378, 379
Krisenmanager	321
Krisenstab	298, 321
Kritikalität.....	446
Kritikalitätsklasse	108
KRITIS	447
Kryptographie.....	236, 447
- ISO/IEC 15946	413
Krypto-Tool	239
KWG.....	406

L

LAN.....	447
Lastenheft	349
LDAP	447
Lebenderkennung.....	223, 293
Lebenszyklus	72, 347
lebenszyklusimmanente	
- Dienstleistungssicherheit	
.....	77
- ITK-Systemsicherheit	77
- Produktsicherheit.....	77
- Prozesssicherheit.....	77
Leerraumdetektion	468
Leistungsmanagement	172
Leistungsvereinbarung.....	172
Leitlinie	54
Leitsatz.....	87
Liberty Alliance	228
Lightweight Directory Access	
Protocol.....	447
Live-Analyse	245
Lizenzmanagement.....	190
Local Area Network.....	447
logging.....	243, 250, 257, 453
Logout	
- simultan.....	253
Lokales Netz	447
Löschttools.....	240
Löschverfahren	
- BSI	240
- DoD 5220.22-M.....	240
- DoD 5220.22-M ECE	240
- Gutmann	240
Löschvorgang	240

M

MAC.....	447
MaLuK.....	409
Makroviren	286
Malware.....	286, 427

-
- MAN 444
 Managed Objects 157
 Managed Services 176
 management by
 - objectives 264
 - walking around 263
 Managementdisziplin
 - Änderungen 185
 - Architektur 246
 - Change 185
 - Compliance 165
 - Datenschutz 166
 - Ereignisse 178
 - Finanzen 176
 - Innovation 259
 - Kapazität 190
 - Konfiguration 188
 - Konformität 165
 - Kontinuität 193
 - Leistungen 172
 - Lizenzen 190
 - Performance 190
 - Personal 261
 - Probleme 184
 - Projekte 177
 - Qualität 177
 - Release 188
 - Risiko 168
 - security 211
 - Service Level 172
 - Wartung 192
 Managementdisziplinen 155
 Mandatory Access Control 447
 man-in-the-middle-Attacken
 464
 MAO 448
 MaRisk 106, 168, 209, 409
 Maßnahmen-Klassen-Matrix
 126
 match on device 293, 294
 Matching
 - One-To-Many 288
 - One-To-One 288
 Maturity Model 383
 - Safety, Security and
 Continuity Management
 383
 - Systems Security
 Engineering 384
 Maximal tolerierbare
 Ausfallzeit 448
 Maximalabstand 317
 Maximale Wiederanlaufzeit
 448
 Maximum Acceptable Outage
 448
 Maximum Tolerable
 Downtime 448
 MBOD 274
 Medium Access Control 447
 Mehrfaktorauthentifizierung
 294
 Mehrfaktoridentifizierung 294
 Merkmal
 - physiologisch 288
 Message Authentication Code
 447
 Metropolitan Area Network
 444
 Mindestanforderungen
 - MaRisk 95
 - Risikomanagement 209
 Mindestgeschäftsbetrieb 448
 Mindestszenarien 91, 448
 Minimalabstand 317
 Mirroring 271, 274
 mission criticality 98
 MKM 126
 Momentaufnahme 368
 monomodal 294
 mTAN 464
 MTBF 448
 MTBSI 448
 MTD 448
 MTTA 448
 MTTR 448

Müllersches V-Quadrupel.. 65,
137
multimodal 294
Multi-Provider-Management
..... 174
multispektral 294
Mustererkennung 281, 449

N

Nacharbeit 449
Nachvollziehbarkeit 148
Namenskonvention 189
narrensicherer Mechanismus
..... 141
NAS 273, 449
NAT 449
NEA 143, 199, 449
nepenthes 283
Nessus 371
Netto-Risiko 63
Network Address Translation
..... 449
Network Attached Storage 273,
449
network centric 273
Network security architecture
- ISO/IEC 18028-2 414
Network security
management
- ISO/IEC 18028-1 26, 414
Netzersatzanlage 143, 199, 449
Netzidentität
- föderierte 229
Netzsegment 148
NEWS
- BCMS 42
- BS 25999-1, 2006 39, 410
- BS 25999-2 42, 410
- COBIT® 4.0 37
- Common Criteria, 2006.. 52

- Digital Signature Services
..... 255
- EDXL-DE 257
- forensische Psychologie 262
- German Signature Law
Profile 256
- GoBS 409
- IEEE 802.11n 436
- ISO/DIS 27799 415
- ISO/IEC 14888-3, 2006.. 413
- ISO/IEC 18028 414
- ISO/IEC 18028-1,2,5, 2006
..... 414
- ISO/IEC 18028-3,4, 2005 414
- ISO/IEC 27002 26, 415
- ISO/IEC 27003 415
- ISO/IEC 27004, FCD 415
- ISO/IEC 27005, FCD 415
- ISO/IEC 27006, 2007 415
- ISO/IEC 27051 415
- IT-GSK 2006 35
- Joint Forum Business
Continuity 418
- Kerberos Token Profile. 251
- NIST 800-94 416
- OASIS™ AdES 416
- OASIS™ Code-Signing
Profile 416
- OASIS™ Digital Signature
Services 416
- OASIS™ EDXL-DE 417
- OASIS™ EPM 417
- OASIS™ SigG Profile ... 417
- OASIS™ SOA 417
- OASIS™ SPML 417
- OASIS™ Timestamping 417
- OASIS™ WSS Kerberos 417
- OASIS™ WSS SAML 417
- OASIS™ WSS SOAP 417
- OASIS™ WSS X.509 417
- OGFSM 258
- OGSA™ 418
- OGSA™ SAML 418

- OGSA™ Security Profile 418
- PAS 77 ITSCM 418
- PostMark Profile... 256, 417
- Sicherheitsstudie <kes>, 2006..... 8
- Telemediengesetz..... 406
- UBL 466
- Username Token Profile 251, 417
- W3C® SOAP 418
- W3C® WSDL 418
- WS-SecureConversation 252, 417
- WS-Trust..... 251, 417
- X.509 Token Profile 251
- XML Code-Signing Profile 256
- XML Timestamping Profile 255, 417
- NFS 273
- NGN 442
- NIDS..... 281
- NIST 449
 - Firewall..... 416
 - IDPS 416
 - IT Security Assessment Framework 416
 - IT Security Engineering Principles 416
 - Risk Management..... 416
 - Security Self-Assessment 416
 - Selecting IT Security Products..... 416
 - Training Requirements 416
- NNIDS..... 282
- Normalbetrieb..... 209
- Notbetrieb..... 194, 449
 - Postvention 194
 - Rückkehr 194
 - Übergang..... 194, 197

- Notfall- und Katastrophenvorsorge ...208, 320
 - Handbuch 320
 - Plan 195
 - Planung 197
- Notfall- und Katastrophenvorsorgeplanu ng.....324
- Notfallkonzept.....209
- Notfalltest.....209
- NP 440

O

- O2M 288
- O2O 288
- OASIS™ 248, 450
 - Advanced Electronic Signature Profiles 416
 - AVDL 256, 416
 - CAP 256, 416
 - Code-Signing Profile 416
 - Common Alerting Protocol 416, 429
 - DSS.....255, 416
 - EDXL-DE.....257, 417
 - EPM 417
 - Kerberos 417
 - RBAC.....457
 - SAML.....417
 - Security Assertion Markup Language.....417
 - Service Oriented Architecture 417
 - Service Provisioning Markup Language.....417
 - SOA 417
 - SOAP 417
 - SPML 417
 - UDDI 417
 - Web Services Security ..417

- Web Services Security	
X.509	417
- XACML	254, 418
OATH	450
Objektschutz	213
- äußerer	214
- innerer	214
OCTAVE®	369
OGC	31
OGF SM	258
OGSA TM	258, 418
- Basic Security Profile ...	418
- SAML	418
- Security Profile	418
OGSI	259
OIA	110, 426
OLA	172, 175
One Time Password	225
open door policy	263
Open Grid Forum SM	258
OpenPGP	450
Operational Impact Analysis	
.....	110, 426
Operational Level Agreement	
.....	172, 175
Operational Risk	410
Opferlamm	280
optischer Sensor	291
Ordnungsmäßigkeit	55
Organisation	75
Organization for the	
Advancement oft Structured	
Information Standards ...	450
OSI-Referenzmodell	450
OTP	225
Out-of-Band-Virtualisierung	
.....	275
Outsourcing	361
- BAKred	410
- FFIEC	408
- Joint Forum	418

P

Paketfilter	278, 451
- mit Zustandstabelle	278
PAP	451, 454
Paperware	188
party	
- asserting	252
- relying	252
PAS 77	418
password	
- cracking	224
- guessing	224
- social hacking	224
Password Authentication	
Protocol	451
Passwort	
- Eigenschaften	332
- ermitteln	224
- erraten	224
- Gebote	331
- probieren	224
- Prüfung	333
- Regeln	331
- Vielfalt	226
Passwortrücksetzung	295
Patchmanagement	186
PDA	5, 239
PDCA-Zyklus	29, 394
PDP	254
Penetrationstest	371
- Black-Box-	371
- Grey-Box-	371
- White-Box-	371
PEP	254
Performancemanagement ..	190
Personal	
- Beschaffung	262
- Betreuung	263
- Einarbeitung	263
- Planung	262
- Prozess	262
- Trennung	264

- Weiterentwicklung..... 263
- Personal Identification
 - Number..... 222
- Personalmanagement..... 261
- Personalprozess 261, 262
- Perspektive
 - finanziell 377
 - Kunden 378
 - Prozesse 379
- Pfadanalyse 147
- PGP 450
- PH 9.330.1 104
- Pharming 5, 451
- Phasen-Ergebnistypen-Tabelle
 - 362
- Phishing 5, 451
- PIC/S PI 011-2..... 408
- PIN..... 222, 452
- pixel per inch..... 294
- PKI 453
- PKIX 454
- Plan-Ist-Vergleich 374
- Plattenspiegelung 271
- Plausibilitätsprüfung 142
- PMBOK® 38
- Poka-Yoke..... 141
- Policy Decision Point 254
- Policy Enforcement Point.. 254
- Politik 54
- POP 452
- POP3..... 452
- POP3s 452
- Portscanning 281
- Post Office Protocol..... 452
- PostMark Profile 417
- Postmarking 256
- Post-Mortem-Analyse 245
- Postvention..... 194
- ppi..... 294
- PPP 451
- Präventivmaßnahme 194
- PRF 440
- Primärspeicher..... 266
- PRIME..... 232
- Prinzip
 - Abstraktion..... 139
 - aufgeräumter Arbeitsplatz
 - 145, 453
 - deny all..... 147
 - Funktionstrennung 146, 437
 - generelles Verbot 147
 - gesperrter Bildschirm... 145
 - grundsätzliches Verbot 147
 - Klassenbildung 140
 - Konsistenz..... 152
 - Konsolidierung 150
 - minimale Dienste 147
 - minimale Nutzung 148
 - minimale Rechte ... 147, 453
 - Namenskonvention 142
 - need-to-use 147
 - Plausibilisierung 152
 - Poka-Yoke..... 141
 - Redundanz..... 142
 - Sicherheitsschalen..... 146
 - Standardisierung 151
 - Vier-Augen- 146
 - Wirtschaftlichkeit..... 139
- Privacy Act..... 106
- Privacy Protection Act
 - Children (COPPA)..... 106
- Problemmanagement 184
- Processware 188
- Produktevaluation 322
- Produktsicherheit
 - lebenszyklusimmanent..77
- Programmierstandards 352
- Projektmanagement..... 177
- PROKom..... 453
- promiscuous mode 282
- PROMSim..... 72
- PROProm..... 453
- PROQuam 453
- PRORim..... 169, 453
- PROSem..... 453

PROSim 72, 75, 130, 453
 PROSom 453
 PROTem 453
 Protocol Stack 447
 Protokollauswertung . 216, 453
 Protokollierung ... 216, 243, 453
 Protokoll-Stack
 - TCP/IP 466
 Protokollstapel 447
 ProTOPSi 72, 453
 Provider
 - Managing, FDIC 408
 - Selecting, FDIC 408
 Provider-Management 172, 174
 - Multi- 174
 Proxy 278
 Prozess 75
 - Architektur 99, 156
 - Begleit- 157
 - ITK-Betriebs- 156
 - Kern- 156
 - Landschaft 99
 - Support- 156
 - Unterstützungs- 156
 Prozesssicherheit
 - lebenszyklusimmanent.. 77
 PS 330 104
 PS 880 104
 Psychologie
 - forensisch 262
 Public Key Infrastructure . 453,
 454
 Public-Key-Verfahren 238
 Pufferüberlauf 355
 Pyramide
 - BCM 11, 61, 445
 - IT 11
 - ITK 11
 - ITK-Governance 11
 - IT-Sicherheit 11
 - Kontinuität 11, 61, 445
 - Management 11
 - Modell 10

 - Projekt 11
 - Qualität 11
 - Risiko 11
 - Service 11
 - Sicherheit 11
 - Sourcing 11, 173
 - Test 11
 - Unternehmen 11
 - Unternehmenssicherheit. 11
 Pyramidenmodell 10

Q

Qualifikationsarchitektur... 297
 Qualifikationsprofil 297
 Qualitätsmanagement 177

R

RADIUS 454
 RAID 270, 455
 - EDAP 272
 - fehlerresistent 272
 - fehlertolerant 272
 - katastrophentolerant ... 272
 - Level 270
 - Neue Kriterien 272
 RAM 454
 Räumlichkeiten 200
 RBAC 457
 RC5™ 237
 real-time reporting 102
 Rechenzentrum 200
 Rechteverwaltung 213
 Records Management 454
 recovery 197
 Recovery 321, 473
 - Plan 195
 - Point Objective 109, 455
 - Time Objective 448
 - Verfahren 324
 Redundancy 455

-
- Redundant Array of
 - Independent Disks 270
 - Inexpensive Disks 455
 - Redundanz 142, 455
 - aktive..... 144
 - Geschwindigkeit... 144, 455
 - heiße..... 144
 - kalte..... 144
 - Latenz 144
 - passive 144
 - Qualität..... 145, 455
 - Quantität..... 143, 455
 - semiaktiv 144
 - strukturell.....142, 143, 455
 - vollständig..... 143
 - warme 144
 - Redundanzgrad 143
 - Regeneration 194
 - Registrierung..... 290
 - Registry 247
 - Reifegradmodell 383
 - Kontrollen 389
 - nach Dr.-Ing. Müller 386
 - Security Maturity Model
 - 386
 - Systems Security Engineering 384
 - Releasemanagement..... 188
 - reliability..... 474
 - Remote access
 - ISO/IEC 18028-4..... 414
 - Remote-Code-Injection 245
 - Replay 337
 - Replay-Attacke 251
 - Report
 - Safety-Security 377
 - Reporting
 - Safety..... 374
 - Safety-/Security..... 374
 - Security 374
 - Repository 247
 - requirements architecture . 132
 - resilience 456
 - Ressource 75
 - Restauration.....473
 - Restore 276
 - Return on Safety, Security and Continuity Investment ...456
 - Return on Security Investment 456
 - Richtlinie 54
 - Benutzerkennung 330
 - Berichtswesen
 - Kontinuitätsmanagement
 - 325
 - Datensicherung 317
 - E-Mail-Nutzung.....307
 - Internet-Nutzung.....310
 - Kapazitätsmanagement311
 - Leseschutz.....335
 - Passwort.....331
 - Protokollierung 336
 - Räumlichkeiten 314
 - WLAN 329, 338
 - Zugriffsschutz 334
 - Zutrittskontrollsystem .337
 - Risiko
 - Aggregation..... 171
 - Architektur 170
 - brutto 63
 - Definition 63
 - Diversifikation..... 171
 - Grenzwert.....90
 - Inventar 171
 - Inventur..... 171
 - Kategorie..... 170
 - Landkarte.....90
 - Managementpyramide. 168
 - netto 63
 - Portfolio 90
 - Pyramide..... 168
 - Strategie.....457
 - Streuung..... 171
 - Transformation 170
 - Risikoanalyse 366, 369, 456
 - Risikodreiklang

- detailliert, nach Dr.-Ing. Müller	63
Risikoinventur	65
Risikomanagement	65, 168, 457
- ISO/IEC 27005, FCD	415
- MaRisk	95
- V-Quadrupel	65
Risikomanagementpyramide	91
Risikopolitik	73
Risikostrategie	136, 137, 457
Risk	
- IT Risk Management Guide	416
- Management Principles	410
- Map	90
- Operational	410
Role Based Access Control	457
Rolle	
- Datenbankadministrator	328
- Netzadministrator	328
- technischer Benutzer	328
RoSI	456
RoSSCI	456
RPO	455
RSA	238
RTO	448

S

Sacrificial Host	280
Safety	131, 153
Safety and Security Engineering	47
Safety, Security and Continuity Engineering ...	47
Safety, Security and Continuity Function Deployment	121

Safety, Security and Continuity Management Maturity Model	383
Safety-Security	
- Audit	78
- Benchmark	380
- Report	377
Safety-Security-Reporting ..	360
SAINT	371
SAML	252, 259, 417, 418
- authority	252
SAN	274, 462
- Fibre-Channel	274
Sanktion	305
Sarbanes-Oxley Act	101
SAS	458
SAS 70	107, 463
SATAN	371
SBOD	274
Scanner	371
Schadensarchitektur	170
Schadensszenarien	111
- Tabelle	111
Schadsoftware	427
Schalenmodell	146
scheduling	157
Schlüssel	
- öffentlicher	238
- privater	238
Schredder	241
Schutzbedarfsanalyse ...	58, 457
- ITK	110
- ITK, Beispiel	113
- Prozesse, Beispiel	113
Schutzbedarfsklassen ...	98, 117
Schutzeinrichtung	56
Schutzgeld	427
Schutzobjekt	56, 457
Schutzobjektklasse	57, 458
Schutzsubjekt	56
Schwachstelle	458
Schwachstellenanalyse	171
Schwachstellenarchitektur ..	171

-
- Schwachstellenstatistik 370
 schwarze Liste 452
 SCSI 461
 SecPAL 259
 Secure Socket Layer 458
 Security 131, 153
 - Engineering 384
 - Manager 349
 Security Appliance 287
 Security Framework
 - W3C® 254
 security incident 360
 Security Incident Response 181
 Security Maturity Model ... 386
 Security Model 452
 Security Profile 418
 - Basic 418
 Security Token 250
 Securitymanagement 211
 Security-Scanner
 - BOSS 371
 - Nessus 371
 - SAINT 371
 - SATAN 371
 Sekundärspeicher 266
 Self Service 231, 295
 Self-Assessment
 - IT Security 370
 Sensibilisierung 264, 458
 Sensor
 - Festkörper 291
 - Flächen- 291
 - optisch 291
 - Streifen- 291
 Serial Attached SCSI 458
 Serverraum 200
 Service
 - Catalogue 172
 - Delivery 162
 - Design 164
 - Desk 178
 - Geber 199
 - Improvement 164
 - Lifecycle 163
 - Operation 164
 - Provider 229, 258
 - Requestor 258
 - Strategy 164
 - Support 162
 - Ticket 227
 - Transition 164
 - Vereinbarung 458
 Service Level
 - Agreement 172, 458
 - Management 172
 - Requirement 172
 Service Oriented Architecture
 151, 246
 Service Provider
 - Managing, FDIC 408
 - Selecting, FDIC 408
 Service-Level-Agreement... 199
 SGB 406
 SGML 450
 Sicherheit
 - Controlling 372
 - ingenieurmäßig 47
 - lebenszyklusimmanent 76,
 149, 195
 - leistungsimmanent 195
 - produktimmanent 195
 - prozessimmanent.. 149, 195
 - Regelkreis 373
 - ressourcenimmanent 149
 Sicherheits-, Kontinuitäts- und
 Risikomanagementprozess
 393
 Sicherheitsanforderungen 73
 - prinzipielle 132
 - Transformation 121
 Sicherheitsarchitektur 74
 - unternehmensspezifisch
 130
 Sicherheitsauditor 78
 Sicherheitsbewusstsein 264
 Sicherheitscontrolling 372

- Sicherheitsdreiklang..... 62
- Sicherheitsselement..... 153
- Sicherheitselemente
 - Kategorien..... 130
- Sicherheitsklasse 108, 233
- Sicherheitskonzept 458
 - generisch..... 74
 - spezifisch 74, 341
- Sicherheitskriterien 57, 108, 459
 - primär 132
 - sekundär 132
- Sicherheitsleitlinie .. 49, 50, 459
- Sicherheitsmanagement 22, 459
 - Prozess 393
- Sicherheitsmaßnahme . 75, 345, 459
- Sicherheitsmodell 452
 - negativ 285
- Sicherheitsniveau.. 88, 368, 460
- Sicherheitsphilosophie..... 460
- Sicherheitspolitik 49, 73, 460
 - ITK, unternehmensweit. 51
 - ITK-System..... 51
 - Leitsatz..... 83, 87
 - nach Dr.-Ing. Müller 53
 - nach ISO/IEC 13335..... 51
 - nach ISO/IEC 15408..... 52
 - nach ISO/IEC 17799..... 52
 - nach ISO/IEC 27001..... 53
 - nach ISO/IEC 27002..... 52
 - nach ITSEC 50
 - nach ITSEC, firmenspezifisch..... 50
 - nach ITSEC, systembezogen..... 51
 - nach ITSEC, technisch.... 51
 - unternehmensweit 51
- Sicherheitsprinzipien 136
- Sicherheitsprozess 393
- Sicherheitspyramide 47, 68, 460
- Sicherheitsregelkreis 78, 373
- Sicherheitsrichtlinien.... 74, 460
- Sicherheitsschalen..... 146
- Sicherheitsschalenmodell...211
- Sicherheitsschirm 211
- Sicherheitsstandards 74, 460
- Sicherheitsstrategie 136, 138, 460
- Sicherheitsstudie 366, 460
- Sicherheitsziele 73, 109, 460
- Sicherheitszone....148, 153, 233
- SigG.....256, 406
 - Profile 417
- Signatur
 - digital.....256
- SigV 256, 406
- Silhouettenerkennung 468
- Simple Mail Transfer Protocol 461
- single logout.....253
- Single Point of
 - Contact 159, 178
 - Failure.....143, 461
 - Security Administration 473
 - Security Control and Administration 221, 473
- Single Point of Failure 194
- Single Sign-on.....227, 260, 461
 - Föderiert 229
 - Kerberos™ 227
 - Passwort-Synchronisation 227
 - Ticket-basiert 227
- Single-Author-Konzept 186
- skill profile 297
- Skript Kiddie.....461
- SKRM.....91
 - Prozess.....394
- SKRMS.....394
- SLA.....172, 458
- SLAD.....372
- SLM.....172
- SLR 172
- Small Computer System Interface 461

-
- Smart Card 429
 - Smartphones 5
 - SMI-S 275
 - SMS 394
 - SMTP 461
 - snapshot 368
 - snapshot copy 274
 - sniffer 461
 - Sniffer 241
 - Sniffer-Interface 281
 - SOA 151, 246, 417
 - SOAP 248, 418
 - Body 248
 - Envelope 248
 - Header 248
 - Intermediary 249
 - Knoten 248
 - Nutzlast 248
 - Zwischenstation 248
 - SOAP Message Security 250
 - SOAP-Umschlag 248
 - social engineering 461
 - social hacking 224
 - Software Test Documentation
..... 410
 - Software Unit Test 410
 - Software Validation 410
 - Software Verification 410
 - Software-Änderung 6
 - Software-Programme
 - digitale Signierung 256
 - Sonden 261
 - Sound Practices 410
 - Sourcing
 - Pyramide 173
 - Ziele 174
 - SOX 101, 408
 - Section 302 101
 - Section 409 178
 - Spam 4
 - over Internet Telephony
..... 471
 - Spam-Mail 285, 472
 - Speicher 266
 - nichtflüchtig 268
 - Pool 274
 - Virtualisierung 274
 - Speicherbereich 148
 - Speicherhierarchie 266
 - Speichermanagement 192
 - Speichermedien 268
 - Speichernetz 274
 - Speichertopologie 272
 - Spezifische
 - Sicherheitskonzepte 74
 - SPICE 418
 - Spionagesoftware 462
 - SpIT 471
 - SPML 417
 - SPoC 178
 - SPoF 461
 - SPSA 473
 - SPSCA 221, 473
 - Spyware 462
 - SQL 462
 - SQL Injection 354, 462
 - SQL-Injektion 462
 - SSCE 47
 - SSCMMM 383
 - SSE-CMM® 384, 418
 - SSL 458, 466
 - Statement on Auditing
 - Standards 463
 - stealth mode 282
 - Steganografie 240, 464
 - Stimmerkennung 295
 - Storage Area Network 274, 462
 - Streifensensor 291
 - Stromausfall 2
 - Structured Query Language
..... 462
 - Subjekt-Recht-Objekt-Modell
..... 236
 - Supportprozess 154, 156
 - sweep 291
 - System

- biometrisch.....	288
Systems Security Engineering	
- Capability Maturity Model	384
System-Sicherheitspolitik	51

T

TAN	464
- eTAN.....	464
- eTAN plus.....	464
- indiziert.....	464
- iTAN.....	464
- mobil	464
- mTAN	464
Tarpit.....	284
Taschenauthentifikator	225, 464
Täuschungsanfälligkeit.....	291
TCP/IP	
- Protokoll-Stack	466
TDDSG	106, 406
TDG	406
TDSV	406
Technikraum	200
Technology Service Providers	
- FFIEC	408
Teerfalle	284
Teergrube.....	284
Telefonbanking.....	295
template	290
Tertiärspeicher	266
Test	464
- Abdeckung	353
- Äquivalenzklasse	353
- Art.....	353
- Ergebnis	353
- Fall	353
- Feld.....	353
- Management	177
- Plan.....	352
- Protokoll	359

- Sequenz	353
- Strategie.....	352
- Szenario	353
- Tiefe	353
- Umfang.....	353
- Umgebung	353
- Vorgehen.....	352
- Ziel	353
TGT	227
Threat.....	426
Ticket Granting Ticket	227
TIGER	372
time stamp	
- Verifizierung.....	255
TKG	406
TKÜV	406
TLS	466
TMG	406
Token	225, 464
Token Profile.....	250
- Kerberos	251
- REL.....	251, 417
- SAML.....	251
- Username	250, 417
- X.509	251
touch	291
TR	440
Transaktionsnummer	464
Transformation.....	73
Transformationsvorgang....	121
Transport Layer Security....	466
Transportsicherung.....	215, 242
Triple DES	237
Tripwire.....	372
Trojan Horse	466
Trojanisches Pferd.....	466
Trust-Center	238
Two-Phase-Commit	205

U

Übertragungssicherung 215,
241, 242

UBL..... 466

Übung 466

- Art 321

- Intervall 321

- Objekt..... 321

- Prozess..... 321

- Ziel 321

UC..... 172, 175

UDDI 248, 417

Underpinning Contract 172,
175

Unified Threat Management
..... 260, 287

Uninterruptable Power
Supply 467

Universal Business Language
..... 466

Universal Description,
Discovery and Integration
..... 248, 417

Unterbrechungsfreie
Stromversorgung.... 199, 467

Unterlagen

- geschäftskritisch 437

Unternehmenspyramide ... 107

Unterstützungsprozess..... 156

Unverfälschtheit 468

Update..... 6

UPS 467

UrhG..... 406

URL 432

USB-Memory-Stick.... 239, 268

USB-Token..... 225

User Help Desk..... 178

USMS..... 20

USV 199, 467

- Line-Interactive 467

- Offline 467

- Online 467

- VFD.....467

- VFI 316, 467

- VI.....467

UTM.....260, 287

V

Validierung 468

VD SG 407

Verbindlichkeit.....468

Verbotsprinzip.....147

Vereinzelungsanlage 468

Verfügbarkeit.....469

Verfügbarkeitsklasse 140

Verfügbarkeitsklassen 469

Verifikation 470

Verkabelung 199

Vernichtung

- Daten 240

- Datenträger.....241

Verschlüsselung ..236, 260, 470

- AES 237

- asymmetrisch.....238

- DES 237

- Druckdaten.....470

- IDEA™ 237

- RC5™ 237

- RSA 238

- symmetrisch 237

- Triple DES.....237

Versorgung 199

Versorgungstopologie 295

Vertrag

- auf Gegenseitigkeit.....470

Vertrauenszirkel.....229

Vertraulichkeit.....470

Vertraulichkeitsstufe 140

Verwundbarkeit 470

VFD 467

VFI.....316, 467

VI.....467

Vier-Augen-Prinzip 146, 471

Virenkennung 286
 Virens Scanner 286
 Virensignatur 286
 Virtual LAN..... 471
 virtual private network
 - ISO/IEC 18028-5 414
 Virtual Tape Library..... 276
 Virtuelle Bandbibliothek.... 276
 Virtuelles LAN..... 471
 Virtuelles Privates Netz 471
 Virus 471
 Vishing..... 471
 vital records..... 437
 VIVA..... 471
 VLAN 471
 Voice over Internet Protocol
 471
 VoIP 471
 VoIP Security Alliance 471
 VOIPSA 471
 Vorgehensmodell..... 11
 VPN 471
 - ISO/IEC 18028-5 414
 VTL 276

W

W3C® 247, 254
 - Security Framework..... 254
 - SOAP..... 418
 - WSDL 418
 - X-KISS 254
 - XKMS 254, 418
 - X-KRSS..... 254
 WAF..... 279
 WAN 472
 Wartung
 - präventiv 193
 Wartungsmanagement 192
 Wassermeldeanlage.... 200, 472
 WBEM 275
 WD..... 440

Web Application Firewall ..279
 Web Services Security.....250
 Webcrawler 472
 WebShield 279
 weiße Liste 452
 Weitverkehrsnetz 472
 Werbe-E-Mail.....472
 Werbesoftware.....472
 whitelist.....285
 Whitelist Model 452
 Wide Area Network.....472
 Wiederanlauf 197, 473
 Wiederanlaufplan 209
 Wiederanlaufzeit
 - maximale.....448
 Wiederaufbereitung....215, 240
 Wiederherstellung..... 194, 473
 Wi-Fi® 436
 WLAN.....436
 WMA.....200, 472
 Workaround..... 178
 Workflow 325
 WpHG.....406
 Write XOR Execute 149
 WSDL.....248, 418
 WSS 250
 WS-SecureConversation....252,
 417
 WS-Trust.....251, 417
 Würmer 286

X

X.1051.....415, 418
 XACML.....254, 418
 XAdES.....256
 X-KISS 254
 XKMS 254, 418
 X-KRSS.....254
 XML 450, 473
 - digital signature 255
 - Enc.....254, 255

- encryption element 255
- Encryption Syntax and Processing 254
- Exclusive Canonicalization 254
- Key Management System 254
- Sig..... 254, 255
- Signature Syntax and Processing 254
- XSS 354, 431

Z

- Zero-Day-Attacke 287, 473
- Zielvereinbarungsprozess . 374
- ZKA 435, 439
- ZKS.....214, 233
- Zufahrtsschutz.....474
- Zugangsschutz 214, 474
 - Basisregel 326
- Zugriffskontrollliste.....474
- Zugriffsschutz 214, 474
- Zutrittskontrollsystem 214, 233
- Zutrittskontrollsystem-
 - Richtlinie 337
- Zutrittsschutz 214, 474
- Zutrittszone 148
- Zuverlässigkeit 474
- Zuwachssicherung 203
- Zwangs-Logout 326
- Zweifaktorauthentifizierung 294
- Zweifaktoridentifizierung .294

Über den Autor

Dr.-Ing. Klaus-Rainer Müller studierte und promovierte in Karlsruhe. Ab 1982 war er als Gruppenleiter der Software-Entwicklung bei einem Hersteller frei programmierbarer Steuerungen tätig, wo er Software spezifizierte und entwickelte sowie Software-Engineering-Methoden einführte.

1986 wechselte er als Senior Software Engineer zur deutschen Tochter eines internationalen System- und Softwarehauses. Hier war er u. a. als Team- und Projektleiter großer, teilweise kritischer Entwicklungsprojekte sowie als Berater tätig und nahm die Positionen Stv. Abteilungsleiter und Key Account Manager wahr.

1993 startete er als Senior Berater und Projektmanager bei der ACG Automation Consulting Group GmbH, einer Unternehmensberatung für Organisation und Informationsverarbeitung in Frankfurt (www.acg-gmbh.de). Als Fachbereichsleiter leitete er den Bereich „Sicherheits- und Qualitätsmanagement“ und beriet in diesen Themen. Seit 1998 leitet er das Fach-Competence-Center (FCC) Unternehmensentwicklung, das heute Organisationsberatung heißt. Von 2003–2005 verantwortete er zusätzlich das FCC IT-Services.

Er befasst sich mit dem IT-Sicherheits-, -Qualitäts-, -Test-, -Service-Level- und -Projektmanagement sowie den betriebswirtschaftlichen Themen Führungssysteme, Prozess- und Strukturorganisation einschließlich Sourcing sowie Organisationsentwicklung. Als Management Berater berät und unterstützt er Kunden beim Aufbau des effizienten und durchgängigen Sicherheits-, Business-Continuity- und Risikomanagements, bei der Entwicklung von Notfall- und Katastrophenvorsorgekonzepten sowie bei der Planung und Durchführung von Notfalltests und -übungen

Er führt u. a. Schutzbedarfsanalysen, Sicherheitsstudien, Reviews und Audits durch, berät und coacht Sicherheitsverantwortliche und moderiert Workshops mit teils stark kontroversen Meinungen. Als Sonderthema gestaltete er im Jahr 1999 den Jahr-2000-Wechsel des IT-Bereichs einer Großbank und begleitete ihn erfolgreich. Darüber hinaus berät er in der breiten Palette der oben genannten Themenbereiche. Zu seinen bisherigen Kunden gehören renommierte Unternehmen u. a. aus den Branchen Banken, Versicherungen einschließlich Sozialversicherungen und Automobil sowie IT-Dienstleister aus den Branchen Banken, Versicherungen und Chemie. Die Projekte sind je nach Themenstellung national, europäisch oder international ausgerichtet.

Er ist Architekt des nach ihm benannten wegweisenden dreidimensionalen Pyramidenmodells und seiner dreidimensionalen Sicherheitspyramide. Den Begriff „Sicherheitspyramide“ prägte er erstmals Mitte der 90er Jahre des vorigen Jahrhunderts und veröffentlichte ihn damals zusammen mit ihrer Darstellung in Artikeln und auf Veranstaltungen. Naturgemäß haben sich ihre Inhalte parallel zu den technologischen, gesetzlichen und regulatorischen Veränderungen in dieser Zeit weiter entwickelt. Darüber hinaus konzipierte und füllte er das auf seinen Ideen basierende zielgruppenorientierte und hoch flexible BCM-Tool der ACG GmbH.

Ende Juli 2003 erschien die erste Auflage seines erfolgreichen Buchs „IT-Sicherheit mit System“, der im August 2005 die zweite Auflage folgte. Sicherheitshierarchie und Lebenszyklus sowie Prozesse, Ressourcen und Organisation sind ebenso wie Kennzahlen seit der 1. Auflage integrative Kernelemente, ebenso wie Muster-Richtlinien u. a. zur E-Mail-Nutzung, zum Computer-Viren-Schutz, zur Datensicherung und zur Notfallvorsorge.

Bisher veröffentlichte der Autor Artikel zur systematischen Pflichtenhefterstellung, zum Software-Engineering, zur Sicherheitspyramide, zum Sicherheits- und Qualitätsmanagement, zur Sicherheit im Software-Lebenszyklus, zum Architekturtrichter, zur prozessorientierten Abnahmeorganisation, zur lebenszyklus- und prozessimmanenten IT-Sicherheit, zum Sourcing mit System, zum Security Engineering, zum Sicherheits- und Risikomanagement, zur genormten Sicherheit sowie zur Biometrie. Außerdem schrieb er die Studie der ACG GmbH zu Biometrie und Smart Cards.

Darüber hinaus hielt er auf Kongressen, Seminaren, Foren und Veranstaltungen verschiedene Vorträge und Präsentationen zu obigen Themenbereichen. Diese behandelten z. B. das Sicherheitsmanagement, Notfalltests und -übungen, das Business Continuity Management, sicherheits- und kontinuieritätsrelevante Aufgaben und Anforderungen des Service Desk, Biometrie, SOA Security und BCM sowie Führungstraining für IT-Sicherheitsexperten.