Heinrich Kersten | Gerhard Klett

Der IT Security Manager

Expertenwissen für jeden IT Security Manager –
Von namhaften Autoren praxisnah vermittelt

2. Auflage

PRAXIS

VIEWEG+
TEUBNER

‹kes›

Heinrich Kersten | Gerhard Klett

Der IT Security Manager

Edition <kes>

herausgegeben von Peter Hohl

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes>– Die Zeitschrift für Informations-Sicherheit (s.a. www.kes.info), die seit 1985 im Secu-Media Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

IT-Sicherheit – Make or Buy
Von Marco Kleiner, Lucas Müller und Mario Köhler

Mehr IT-Sicherheit durch Pen-Tests
Von Enno Rey, Michael Thumann und Dominick Baier

ITIL Security Management realisieren
Von Jochen Brunnstein

IT-Sicherheit kompakt und verständlich
Von Bernhard C. Witt

IT-Risiko-Management mit System
Von Hans-Peter Königs

Praxis des IT-Rechts
Von Horst Speichert

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz
Von Heinrich Kersten, Jürgen Reuter und Klaus-Werner Schröder

Datenschutz kompakt und verständlich
Von Bernhard C. Witt

Profikurs Sicherheit von Web-Servern
Von Volker Hockmann und Heinz-Dieter Knöll

Heinrich Kersten | Gerhard Klett

Der IT Security Manager

Expertenwissen für jeden IT Security Manager –
Von namhaften Autoren praxisnah vermittelt

2., aktualisierte und erweiterte Auflage

Mit 21 Abbildungen

herausgegeben von Heinrich Kersten und
Klaus-Dieter Wolfenstetter

PRAXIS

VIEWEG+
TEUBNER

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.

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 2005
2., aktualisierte und erweiterte Auflage 2008

Lektorat: Sybille Thelen | Andrea Broßler

Der Vieweg+Teubner Verlag ist ein Unternehmen von Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0429-7

Vorwort

Vorwort zur 2. Auflage

Nachdem die Erstauflage des Buches im Herbst 2007 vergriffen war, stellte sich die Frage nach einem unveränderten Nachdruck oder der Herausgabe einer überarbeiteten Fassung.

Verlag und Autoren haben sich für Letzteres entschieden: Eine Überarbeitung und Ergänzung erschien unter anderem deshalb sinnvoll, weil mit dem Erscheinen der ISO 27001 – auch in deutscher Sprache – viele Unternehmen eine neue Herausforderung sehen, andererseits einige wichtige technische Themen wie Internet-Sicherheit, Risikoanalyse und IT Compliance bei der Erstauflage nur beschränkt berücksichtigt wurden.

Zwischenzeitlich eingegangene Kritiken und Vorschläge der Leser sind ebenfalls in die Überarbeitung eingeflossen: hierfür herzlichen Dank.

Dem Verlag, seinem Programmleiter Herrn Günter Schulz und dem Lektorat danken die Autoren für die Unterstützung bei der zweiten Auflage dieses Buches.

Im Februar 2008, Dr. Gerhard Klett, Dr. Heinrich Kersten

Vorwort zur 1. Auflage

Das vorliegende Buch richtet sich an Leser, die sich in das interessante Gebiet der Informationssicherheit einarbeiten möchten.

Dieses Gebiet ist z. T. unter anderen Überschriften wie IT-Sicherheit (IT Security), Datensicherheit, Informationsschutz bekannt und berührt auch Themen wie den Datenschutz, das Qualitätsmanagement, die Ordnungsmäßigkeit der Datenverarbeitung.

Sicherheit der Information und Sicherheit bei der Verarbeitung von Daten sind heute keine Ziele mehr, für die man Werbung betreiben müsste. Jeder hat mehr oder weniger eigene Erfahrungen mit diesen Themen gemacht – sei es als Geschädigter oder als Verantwortlicher. Deshalb wollen wir uns hier ersparen, Horror-Szenarien zu beschreiben – man kennt sie hinlänglich aus entsprechenden Publikationen.

Im Vordergrund stehen heute mehr die Fragen,

– wie man die gewünschte Sicherheit erreichen kann,

– wie man gegenüber Partnern, Kunden, Aufsichtsbehörden und Banken die eigene Sicherheit nachweisen kann,

– ob es einen *Return on Security Investment* (ROSI) gibt und wie man ihn ggf. erreicht.

Im Grunde muss sich heute jede Institution, die schützenswerte Informationen besitzt und Daten sicher verarbeiten will, mit diesem Thema beschäftigen: Es ist zu einem wichtigen Faktor der Unternehmensvorsorge geworden. Dabei hat sich die Erkenntnis durchgesetzt, dass sich Sicherheit nicht allein aufgrund technischer Vorkehrungen einstellt, sondern dass man Sicherheit „managen" muss, woraus sich beinahe zwangsläufig ergibt, dass „Sicherheit" kein Zustand ist, sondern eine kontinuierliche Aufgabe darstellt.

Dies hat dazu geführt, dass in vielen Institutionen ein Sicherheitsmanagement eingerichtet worden ist, das sich in Gestalt eines *IT-Sicherheitsbeauftragten* oder eines entsprechenden Gremiums der Sicherheitsthematik annehmen soll – aber wie?

Das Thema der Informationssicherheit ist ein sehr komplexes – sowohl vom Umfang als auch vom methodischen Zugang her. Wichtige Aspekte betreffen die rechtliche Sicherheit, Fragen der organisatorischen und personellen Sicherheit, die Infrastruktursicherheit, die Sicherheit der IT-Systeme und Netze, die Sicherheit von Geschäftsprozessen.

Es existieren unzählige Vorschläge, sogar umfangreiche Kataloge für Sicherheitsmaßnahmen: Die Bewertung solcher Maßnahmen im Hinblick auf die Eignung und Sicherheit in einem speziellen Einsatzszenario stellt eine nicht zu unterschätzende Herausforderung dar.

Sicherheitskonzept

Eine wichtige Funktion kommt dabei dem so genannten *Sicherheitskonzept* zu, das alle Analysen und Entscheidungen, die die IT-Sicherheit betreffen, enthalten soll. Um dieses meist umfangreiche Dokument rankt sich in der Praxis ein ganzes Bündel von begleitenden Dokumenten – sehr zum Leidwesen der Beteiligten, da „Paperware" einerseits meist Schwerstarbeit ist und andererseits allein noch gar nichts bringt.

Von der methodischen Seite ist das Schreiben von aussagekräftigen Sicherheitskonzepten in diesem Gebiet ein Kardinalproblem: Individuelle Risiken, die Wirksamkeit von Gegenmaßnahmen und das verbleibende Restrisiko können meist nicht berechnet, sondern bestenfalls aus der Erfahrung „geschätzt" werden.

Wer in dieses Gebiet neu einsteigt, kann schnell den Überblick verlieren und wird auch nach vielen Jahren Berufserfahrung immer wieder Neues entdecken. Dennoch gilt es gerade zu Beginn, sich auf das Wesentliche zu konzentrieren.

Sicherheitsmaßnahmen gibt es in großer Zahl und unterschiedlicher Ausprägung. Ihre detaillierte Behandlung würde den Rahmen dieses Buches sprengen. Es musste deshalb eine Auswahl getroffen werden: Als Orientierung dienten mehrtägige Einführungsseminare in die Aufgaben des IT Security Managers, die die Autoren in den vergangen Jahren zahlreich durchgeführt haben (und noch durchführen). Das Feedback der Teilnehmer hat dabei vielfältige Anregungen zur Überarbeitung von Methodik und Didaktik gegeben.

Zielgruppe

Das vorliegende Buch ist speziell auf die Belange von Einsteigern zugeschnitten; es kann aber auch dem erfahrenen Praktiker einige neue Aspekte und Sichtweisen näher bringen – wenn er auch zwangsläufig manche Themen vermissen wird.

An vielen Stellen in diesem Buch ist von „Unternehmen“ die Rede; alle Ausführungen gelten selbstverständlich auch für andere Formen von Institutionen wie Behörden, Verbände, Vereine, usw.

An einigen Stellen in diesem Buch geben wir bei neuen Begriffen die einschlägige englische Übersetzung an, um das Lesen von weiterführender Literatur in englischer Sprache zu erleichtern.

Danksagung

Für viele anregende Diskussionen möchten die Autoren vor allem Herrn Christoph Fischer (BFK edv-consulting GmbH), Herrn Manfred Hübner (WestLB AG), Herrn Dr. Gerald Spiegel (SerCon GmbH) und Herrn Klaus-Dieter Wolfenstetter (Deutsche Telekom AG, Laboratories) danken.

Dem Vieweg-Verlag und seinem Programmleiter Herrn Dr. Reinald Klockenbusch möchten die Autoren für die professionelle Unterstützung bei der Herstellung dieses Buches und vor allem für die große Geduld danken, da eigentlich alles viel schneller gehen sollte…

Im August 2005, Dr. Gerhard Klett, Dr. Heinrich Kersten

Inhaltsverzeichnis

1 Zur Motivation

Insgesamt ist es eine nicht zu unterschätzende Herausforderung, gute IT-Sicherheitskonzepte zu schreiben und die IT-Sicherheit qualifiziert zu managen. Man kann sich diese Aufgabe aber auch unnötig schwer machen: Betrachten wir einige Erfahrungen aus der Praxis von Sicherheitsberatern:

- Unklare Verantwortlichkeiten bezüglich der IT-Sicherheit sowie eine schwammige Abgrenzung zu anderen Aufgaben im Unternehmen erschweren ein zielführendes Sicherheitsmanagement, machen es teilweise sogar unmöglich.
- Operiert man mit unklaren Begriffen, so versteht jeder Beteiligte etwas anderes, es gibt langwierige, ineffektive Diskussionen unter den Betroffenen, die Analysen werden unterschiedlich interpretiert, das Ergebnis ist in alle Richtungen auslegbar und damit nichtssagend.
- Verwendet man für den Sicherheitsprozess Vorgehensmodelle, die hoch-wissenschaftlich angelegt oder im Gegenteil zu banal gestrickt sind, ist das Ergebnis praxisfern, nutzlos und bestenfalls für die „Schublade“ geeignet.
- Das leidige Thema „Dokumentation“: Man kann bei der Vielzahl von Dokumenten, Listen und Informationen in der Praxis leicht den Überblick verlieren, wenn man hier ohne eine gute Struktur und Planung einsteigt.
- Macht das Sicherheitsmanagement nur Vorgaben, ohne die Einhaltung derselben zu kontrollieren, hat man eine klassische Management-Aufgabe nicht erfüllt und damit grob fahrlässig gehandelt.

Es kann deshalb nur dringend empfohlen werden,

- eine klare Aufgabenbeschreibung für das IT-Sicherheitsmanagement zu erstellen und die Schnittstellen zu anderen Verantwortlichkeiten festzulegen,
- ein einheitliches Begriffsverständnis zwischen den Beteiligten herzustellen und dieses schriftlich festzuhalten, etwa in Form eines Glossars, das allen weiteren Dokumenten vorangestellt wird,

– erprobte, möglichst standardisierte Vorgehensmodelle heranzuziehen und nutzbringend anzuwenden,

– im Sicherheitsprozess regelmäßige Überprüfungen der Vorgaben und ihrer Einhaltung vorzusehen.

Eine wichtige Entscheidung gleich zu Beginn betrifft die Frage, ob man mit der Sicherheitsdiskussion im Unternehmen auf der Ebene von

– IT-Systemen und Netzen,

– IT-Anwendungen oder gar

– „ganz oben" bei den Geschäftsprozessen

einsteigen möchte. Grundsätzlich sind die IT und die Unternehmensnetze „Werkzeuge", die die Geschäftstätigkeit des Unternehmens unterstützen – das eigentliche Problem ist damit die Sicherheit der Geschäftsprozesse. Bei deren Diskussion kommt man natürlich automatisch auch zur klassischen IT-Sicherheit von Daten, Systemen, Netzwerken und Anwendungen, aber dies allein ist nicht ausreichend: Ein „ganzheitlicher" Ansatz betrachtet auch die Anteile an Geschäftsprozessen, die ohne IT erledigt werden und je nach Lage einen signifikanten Beitrag zur Sicherheit und zur Unsicherheit liefern können.

Inzwischen gibt es einige Jahrzehnte an Erfahrung auf dem Gebiet der IT-Sicherheit und der Informationssicherheit, so dass es nicht verwundert, wenn Sicherheitsmanagement und Sicherheitsmaßnahmen Gegenstand von Standards und vergleichbaren Vorgaben geworden sind.

Bei den Sicherheitsverantwortlichen in den Unternehmen findet man zwei unterschiedliche Gruppen vor: Während die eine im Schwerpunkt sehr Maßnahmen-orientiert denkt, sieht die andere mehr den Sicherheitsprozess und sein Management im Vordergrund.

Dies ist eigentlich gar kein Gegensatz – die „Wahrheit" ist: Man braucht beides. Ein Prozess lässt sich natürlich international viel leichter standardisieren als etwa ein Maßnahmenkatalog, dessen Inhalt schnell „veraltet" ist und der bei der Vielzahl von Anwendungen der IT immer nur Ausschnitte abdecken kann.

ISO 27001

Es verwundert deshalb nicht, dass ausgehend von dem British Standard (BS) 7799 der internationale Standard ISO 27001 entstanden ist, der die IT-Sicherheit im Kern als einen Management-Prozess sieht. Für alle zu behandelnden Sicherheitsthemen werden zwar (im Anhang des Standards) Maßnahmenziele und An-

forderungen angegeben – die Auswahl von geeigneten Einzelmaßnahmen bleibt jedoch dem Anwender überlassen.

Ein Vergleich zeigt, dass eine Reihe von Management-Elementen nicht nur im ISO 27001, sondern auch in anderen Management-Standards wie dem Qualitätsmanagement (ISO 900x) und dem Umweltschutz-Management (EN 1400x) auftreten. Dieser gemeinsame Querschnitt aller bekannten Management-Standards beinhaltet das so genannte PDCA-Modell. Andere Verfahrenselemente wie z. B. das Änderungsmanagement (Change Management) und die Dokumentenlenkung sind typische QM-Verfahren und werden für die Sicherheit analog angewendet. Hieraus ergibt sich auch die Möglichkeit, gemeinsame Management-Strukturen für diese Themen im Unternehmen aufzubauen und somit einen ersten Beitrag zum Return on Security Investment zu liefern.

Grundschutzhandbuch

Parallel dazu hatte sich mit dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Grundschutzhandbuch in Deutschland ein Quasi-Standard entwickelt, dessen Kern letztlich die Maßnahmen-orientierte Sichtweise ist. Dieses umfangreiche und regelmäßig aktualisierte Werk stellt im Grunde einen kommentierten Maßnahmenkatalog dar, dessen Anwendbarkeit nach Aussage des BSI auf den „normalen“ Schutzbedarf beschränkt ist.

Nachdem lange Zeit – vor allem in Deutschland – eine Kontroverse zwischen beiden Sichtweisen der IT-Sicherheit bestand, hat man inzwischen eine Kehrtwendung vollzogen: Die Management-Elemente der IT-Sicherheit sind aus dem IT-Grundschutzhandbuch herausgelöst und in Form von BSI-Standards veröffentlicht worden. Dabei wurde auf Konformität zu den entsprechenden Elementen der ISO 27001 geachtet.

Gefährdungs- und Maßnahmenkataloge sind nunmehr eigenständig; letztere sind insbesondere dazu geeignet, eine Reihe von Vorgaben aus dem Anhang A des Standards mit Einzelmaßnahmen zu versehen (nur für den „normalen“ Schutzbedarf“).

Als weiterer BSI-Standard ist eine Vorgehensweise für eine „Risikoanalyse“ veröffentlicht worden, die für die Schutzbedarfe „hoch“ und „sehr hoch“ anwendbar ist und auf der Grundschutzmethode aufbaut.

Wir wollen die genannten Werke hier nicht in anderer Formulierung wiedergeben, sondern eher eine generische Sichtweise der IT-Sicherheit und ihres Managements bringen, die von Einsteigern wie auch erfahrenen IT-Sicherheitsbeauftragten leicht in

die Praxis umgesetzt werden kann. Will man ggf. später die Konformität zum Standard ISO 27001 (mit oder ohne Grundschutz) oder zu anderen Standards herstellen, wird dies mit geringem Zusatzaufwand erreichbar sein. In diesem Zusammenhang sei auf /KRS2008/ verwiesen.

2 Sicherheitsmanagement – Konzeptionelles

2.1 Sicherheit als Management-Prozess

Einige wichtige Erfahrungen wollen wir diesem Kapitel voranstellen:

– Eine absolute Sicherheit[1] gibt es in der Realität nicht.

Man ist von diesem Idealzustand immer ein gutes Stück entfernt. Das sollte auch so bleiben, weil andernfalls die Kosten für die Sicherheit nicht mehr tragbar wären. Wir sprechen deshalb von einem gewünschten bzw. erreichten Sicherheitsniveau, d. h. Sicherheit ist eine Frage von „mehr“ oder „weniger“.

– Ein erreichtes Sicherheitsniveau bleibt nicht auf Dauer bestehen.

Dies hat seinen Grund darin, dass immer wieder bisher nicht bekannte Sicherheitslücken bzw. Schwachstellen in der Technik entdeckt werden und neue Angriffstechniken entstehen – aber auch neue Sicherheitsvorkehrungen entwickelt werden. Sicherheit ist also zeitabhängig: Was heute als sicher gilt, kann unter Umständen in Kürze als unsicher angesehen werden.

– Ein erreichtes Sicherheitsniveau gilt nur für ein genau abgegrenztes Szenario.

Anwendungsbereich

Wenn man Sicherheit konzipiert, geht man so vor, dass zunächst der Gegenstand festgelegt wird, auf den sich das Konzept beziehen soll, d. h. die zu betrachtenden Systeme, Netze, Geschäftsprozesse werden angegeben.

Vor allem in Standards verwendet man anstelle von „Szenario“ auch gerne den Begriff „Anwendungsbereich“ oder das englische Wort „Scope“.

Änderungen des Anwendungsbereiches sind in der Praxis an der Tagesordnung: Häufige Änderungen an den Geschäftsprozessen eines Unternehmens, seiner IT und den betriebenen Anwendun-

---

1 In diesem Abschnitt verwenden wir „Sicherheit“ stellvertretend für IT-Sicherheit, Informationssicherheit, etc. Eine genauere Festlegung solcher Begriffe erfolgt in einem späteren Kapitel.

gen machen es aber den Sicherheitsverantwortlichen nicht leicht: Ändert man den Anwendungsbereich – und sei es nur marginal – kann dies jede denkbare Auswirkung auf die Sicherheit haben: Sie kann sich erhöhen, gleich bleiben, aber auch verringern.

– Sicherheit und Sicherheitsmanagement funktionieren nur in einem sensibilisierten Umfeld.

Das beste Sicherheitskonzept und die teuersten Maßnahmen kommen nicht richtig zum Zug, wenn es bei den Mitarbeitern und der Leitungsebene an Problembewusstsein und Problemwissen („Awareness") fehlt.

Prozess

Aus den zuvor dargestellten Überlegungen erkennt man, dass Sicherheit im wahrsten Sinne eine „Variable" ist und ein permanentes Bemühen erfordert. Sicherheit ist also kein erreichbarer Zustand, sondern ein Prozess. Ziel des Prozesses ist es, ein gewünschtes Sicherheitsniveau erstmalig zu erreichen, dieses aufrechtzuerhalten und die Sicherheit insgesamt weiterzuentwickeln bzw. zu verbessern.

Damit haben wir auch die Aufgabe des Sicherheitsmanagements umrissen.

Verbesserungspotenzial

Das Verbessern der Sicherheit *kann*

– die Veränderung des Anwendungsbereichs betreffen: Man „sichert" beispielsweise zunächst nur bestimmte Organisationseinheiten des Unternehmens und nimmt dann sukzessive weitere hinzu, bis man die gewünschte „Ausbaustufe" erreicht hat,

– eine Anpassung des Sicherheitsniveaus an eine reale Gefährdungslage zum Ziel haben: Man beginnt mit einem bestimmten Sicherheitsniveau und passt dieses von Zeit zu Zeit an die aktuelle Gefährdungslage an; dabei kann es um ein Erhöhen oder Verringern des Sicherheitsniveaus gehen,

– die Erhöhung der Sensibilität für die Sicherheit im Unternehmen zum Ziel haben,

– den Prozess des Sicherheitsmanagements als solches betreffen.

2.2 Das PDCA-Modell

Wir brauchen nun eine Art „Vorgehensmodell", um das Verbesserungspotenzial sukzessive ausschöpfen zu können. Genau dies leistet das so genannte *PDCA-Modell*. Die Buchstaben stehen für

die englischen Wörter **P**lan, **D**o, **C**heck, **A**ct. Dahinter verbirgt sich ein Management-Modell, mit dem man

- die Erreichung von Zielen – hier das gewünschte Sicherheitsniveau – zunächst plant bzw. konzipiert (*plan*),
- die Planung bzw. Konzeption realisiert (*do*),
- über eine gewisse Zeit Erfahrungen mit der Realisierung macht, d. h. überprüft, ob die Konzepte sich in der Praxis bewähren bzw. wo es Probleme gibt (*check*),
- aus den gewonnen Erkenntnissen und anderen zwischenzeitlich gestellten neuen Anforderungen notwendige Veränderungen ableitet (*act*).

Diese 4 Phasen des PDCA-Zyklus sind als Regelkreis zu verstehen, d. h. nach der Phase *act* steigt man wieder in die Phase *plan* ein, um die als notwendig erkannten Änderungen zu planen, danach in die Phase *do*, usw.

Bei der Phase *act* werden neben den Erkenntnissen der Phase *check* auch andere zwischenzeitlich gestellte neue Anforderungen berücksichtigt. Hiermit reagiert man auf die Erfahrung, dass im laufenden Prozess oft der Anwendungsbereich oder das Sicherheitsniveau angepasst werden soll oder auch nur neue Sicherheitserkenntnisse zu berücksichtigen sind.

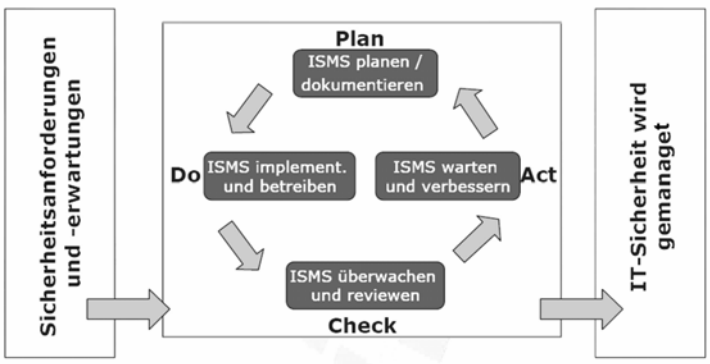

Abbildung 1: PDCA-Zyklus in der IT-Sicherheit

ISMS

Man erkennt sofort, dass dieses Modell im Grunde für das Management jedes Themas geeignet ist. Es findet deshalb in zunehmendem Maße in allen Management-Standards Anwendung[2]. Die Abbildung 1 konkretisiert das PDCA-Modell für das „Informationssicherheits-Management-System" (ISMS).

Wie und wo soll nun das PDCA-Modell angewendet werden?

Betrachten wir die ideale Situation, dass von der Unternehmensleitung das Thema IT-Sicherheit aufgegriffen, ein Sicherheitsmanagement eingerichtet und diesem die interne Verantwortung für die Sicherheit übertragen wird. Auf beiden Ebenen – der Leitung und dem Sicherheitsmanagement – ist nun das PDCA-Modell zu realisieren:

Leitungsebene

Bei der Leitung besteht *plan* darin, eine Zielvorgabe für die Sicherheit zu geben; dies solle schriftlich geschehen, und zwar mit der so genannten „Sicherheitsleitlinie". Die Phase *do* besteht darin, das Sicherheitsmanagement einzurichten und damit zu beauftragen, die Sicherheitsleitlinie umzusetzen. In der Phase *check* prüft die Leitung aufgrund der Berichte des Sicherheitsmanagements und ggf. eigener Erkenntnisse, ob die Zielvorgabe umgesetzt worden ist und ob es Probleme in der Anwendung gegeben hat. Aus dem Ergebnis werden Schlüsse über notwendige Anpassungen der Sicherheitsleitlinie getroffen (*act*).

Management-Bewertung

Praktisch geschieht dies alles dadurch, dass die Leitung den PDCA-Zyklus in regelmäßigen Sitzungen abarbeitet und über die Ergebnisse entsprechende Aufzeichnungen macht. Themen dieser Sitzungen sind die Berichte des Sicherheitsmanagements, eigene Erkenntnisse über die Sicherheit des Unternehmens oder von Dritten, ebenso wesentliche Änderungen der Gesetzeslage oder neue geänderte Sicherheitsanforderungen aus aktuellen Kundenverträgen.

Der zentrale Besprechungspunkt ist dabei regelmäßig die *Bewertung* der Sicherheitslage des Unternehmens und die *Bewertung* der Wirksamkeit des Sicherheitsmanagements sein, weshalb

---

2 z. B. beim Quality Management (ISO 900x), Umweltschutz-Management (EN ISO 1400x), Sicherheitsmanagement (ISO 27001); es findet aber auch implizit Anwendung beim Management von sicherheitskritischen Organisationseinheiten; ein Beispiel hierfür sind Vorgaben in einer Schweizer Richtlinie zum Sicherheitsmanagement beim Betrieb von Trust Centern oder den entsprechenden Vorgaben des Standards ETSI 101.456.

im Standard ISO 27001 auch von einer *Management-Bewertung* die Rede ist.

Im Ergebnis dieser Sitzungen kann eine Entlastung des Sicherheitsmanagements erfolgen oder diesem eine geänderte Sicherheitsleitlinie zugeleitet werden mit der Vorgabe, die Änderungen umzusetzen.

Sicherheitsmanagement

Auf der Ebene des Sicherheitsmanagements wird ebenfalls nach PDCA gearbeitet: Mit der Zielvorgabe der Sicherheitsleitlinie als Input wird die gewünschte Sicherheit konzipiert (*plan*), d. h. es entsteht ein „Sicherheitskonzept", oder es werden Anpassungen an einem existierenden Sicherheitskonzept vorgenommen.

Die Umsetzung dieses Konzeptes geschieht in der Phase *do*. Alle Erfahrungen aus der Praxis und aus regelmäßigen Überprüfungen werden aufgezeichnet (*check*). In der Phase *act* werden die gesammelten Aufzeichnungen – in Verbindung mit sonstigen Erkenntnissen – ausgewertet und Handlungsvorschläge zur Verbesserung der Sicherheit abgeleitet. Das Ergebnis der Phase *check* wird der Leitung mitgeteilt. Stimmt diese dem Ergebnis zu, plant das Sicherheitsmanagement die Umsetzung der Verbesserungsvorschläge und steigt damit wieder in die Phase *plan* ein…

Auch beim Sicherheitsmanagement sollte man sich konsequent am PDCA-Modell orientieren, folglich regelmäßig Sitzungen mit den Beteiligten anberaumen, um sukzessive die 4 Phasen abzuarbeiten. Gegenstand der Besprechungen sind u. a. neue Sicherheitserkenntnisse und eventuelle Sicherheitsvorkommnisse, die analysiert und bewertet werden müssen. Die Ergebnisse solcher Besprechungen sind natürlich aufzeichnen!

In welchem Abstand sind solche Besprechungen durchzuführen? Sie könnten z. B. quartalsweise durchgeführt werden mit dem Ziel, den vollen PDCA-Zyklus einmal pro Jahr bearbeitet zu haben. Je nach Erfordernissen kann man diese Abstände auch verlängern oder verkürzen. In den Standards finden sich hierzu keine bindenden Vorgaben. Ungeachtet dessen können z. B. gravierende Sicherheitsvorfälle Anlass bieten, solche Besprechungen anzuberaumen.

Man erkennt, dass durch Einhaltung dieses Vorgehensmodells das Verbesserungspotenzial sukzessive ausgeschöpft und somit die Sicherheit Schritt für Schritt verbessert werden kann.

Konkretisierung

Das PDCA-Modell wollen wir nun eine Ebene tiefer konkretisieren, indem wir die relevanten Tätigkeiten für die Leitung und das

Sicherheitsmanagement zusammenstellen. Beginnen wir mit der Leitungsebene:

Tabelle 1: PDCA für die Leitungsebene

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen	
Plan3	Sicherheitsleitlinie als Zielvorgabe erstellen (lassen)	Sicherheitsleitlinie ggf. anpassen / überarbeiten (lassen)
Plan4	Sicherheitsleitlinie formell in Kraft setzen	Ggf. geänderte Sicherheitsleitlinie formell in Kraft setzen
Do		
Do1	Sicherheitsmanagement einrichten	ggf. Sicherheitsorganisation anpassen
Do2	Ressourcen bereitstellen	Ressourcen ggf. anpassen
Do3	Auftrag an das Sicherheitsmanagement: Sicherheitsleitlinie umsetzen, regelmäßig Berichte für die Leitungsebene erstellen	
Check		
Check1	Berichte des Sicherheitsmanagements prüfen	
Check2	sonstige Erkenntnisse einbringen	
Act		
Act1	Informationen analysieren	
Act2	Verbesserungspotenzial feststellen	
Act3	Vorschläge des Sicherheitsmanagements prüfen / genehmigen bzw. ablehnen	

Einige Anmerkungen zu den einzelnen Punkten:

Plan1/2

Als Teil der Phase *plan* haben wir zwei neue Aktivitäten einbezogen:

– die Sensibilisierung der Leitungsebene für die Informationssicherheit,
– die Beschaffung weiterer Informationen, um die folgenden Schritte qualifiziert angehen zu können.

Dies erscheint notwendig, weil oft nur ein rudimentäres Verständnis für das Thema und seine Strukturen gegeben ist. Weitere Informationen hierzu finden Sie im Abschnitt „2.3 Unverzichtbar: Sensibilisierung, Schulung, Training".

Plan3 Die Sicherheitsleitlinie ist das zentrale Vorgaben-Dokument der Leitungsebene für die Informationssicherheit im Unternehmen. Es stellt einerseits den wichtigen Input für das vom Sicherheitsmanagement zu erstellende Sicherheitskonzept dar, andererseits ist es auch eine Zielvorgabe für alle Mitarbeiter des Unternehmens. Weitere Informationen finden Sie im Kapitel „6. Die Sicherheitsleitlinie".

Plan4 Die Sicherheitsleitlinie ist erstmalig und ebenso nach Änderung per Unterschrift in Kraft zu setzen. Sie muss anschließend den Mitarbeitern des Unternehmens bekannt gegeben werden.

Check2 In dieser Teilphase geht es um sonstige Erkenntnisse der Leitungsebene – z. B. aus eigenen Beobachtungen und Sicherheitsvorfällen oder Mitteilungen Dritter.

Kommen wir nun zu den PDCA-Aktivitäten des Sicherheitsmanagements:

Tabelle 2: PDCA für das Sicherheitsmanagement

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	eigene Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen, ggf. eigene Schulung	
Plan3	Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren	die geänderte Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan4	Sicherheitskonzept und Begleitdokumente erstellen (lassen)	Sicherheitskonzept und Begleitdokumente ggf. anpassen und überarbeiten (lassen)
Plan5	Abstimmung und Genehmigung des Sicherheitskonzeptes und der Begleitdokumente	Abstimmung und Genehmigung nur der Änderungen bzw. Neuerungen
Do		
Do1	Sicherheitskonzept (resp. Änderungen) durch zuständige Fachabteilungen umsetzen lassen	
Do2	Umsetzung überwachen	
Do3	Maßnahmen aus den Bereichen Sensibilisierung, Schulung, Training aufsetzen.	
Do4	Sicherheitskonzept in Kraft setzen	
Do5	Sicherheitsvorfälle managen	
Check		
Check1	Praxis überprüfen	
Check2	Sicherheitsvorfälle auswerten	
Check3	sonstige Erkenntnisse einbringen	
Act		
Act1	Schlussfolgerungen ziehen	
Act2	Verbesserungspotenzial feststellen, Berichte an die Leitung	

Plan 3

Eher selten kommt der Fall vor, dass die Leitungsebene die Sicherheitsleitlinie selbst erstellt, vielmehr erhält das Sicherheitsmanagement den Auftrag, einen Entwurf zu erstellen. Wesentlich ist aber, dass die Leitung die Sicherheitsleitlinie in Kraft setzt. Erst dann sollte sie als Input für das Sicherheitsmanagement gelten.

Plan4

Das Sicherheitskonzept ist das zentrale Dokument für das Sicherheitsmanagement. Es sollte vollständig, in sich konsistent und nachvollziehbar sein. Weitere Informationen zum Sicherheitskon-

zept finden Sie im Kapitel „8. Das Sicherheitskonzept“. Hinweise zu den Begleitdokumenten und zum Aufbau der Sicherheitsdokumentation finden Sie im Abschnitt „2.4 Management der Dokumentation“.

Plan5 Dieser Punkt *Plan5* muss bei der Planung der Schritte berücksichtigt werden, weil er erfahrungsgemäß immer einen hohen zeitlichen Verzug mit sich bringt.

Do1/Do2 Nach der Genehmigung des Sicherheitskonzeptes müssen die dort aufgeführten Maßnahmen sukzessive umgesetzt werden. Dabei ist es *nicht* die Aufgabe des Sicherheitsmanagements, die Umsetzung ganz oder in Teilen selbst vorzunehmen. Vielmehr ist dies die Aufgabe der zuständigen Fachabteilungen, etwa der Personalabteilung für personelle Maßnahmen, der IT-Abteilung für IT-bezogene Maßnahmen, usw.

Das Sicherheitsmanagement überwacht diese Umsetzungen in dem Sinne, dass eine genaue Übereinstimmung zwischen Sicherheitskonzept und Praxis erzielt wird. Um dies zu erreichen ist es sinnvoll, die ausführenden Fachabteilungen mit einem Formular auszustatten, mit dem für jede Maßnahme

- entweder die korrekte Umsetzung bestätigt wird,
- oder ggf. aufgetretene Probleme mit entsprechenden Lösungsvorschlägen an das Sicherheitsmanagement berichtet werden.

Do3 Hier geht es um Maßnahmen für die *Mitarbeiter* als Zielgruppe: Es muss eine ausreichende Sensibilität für die Informationssicherheit vorhanden sein und aufrechterhalten werden. Schulungsmaßnahmen betreffen die vorgesehenen Sicherheitsmaßnahmen und deren Nutzung bzw. Einsatz. Training bezieht sich auf die Tätigkeiten sicherheitskritischer Rollen. Nähere Informationen finden Sie im Abschnitt „2.3 Unverzichtbar: Sensibilisierung, Schulung, Training“.

Do5 Beim Management von Sicherheitsvorfällen geht es um die drei Aktivitäten *Erkennen*, *Melden* und *Bearbeiten* von Sicherheitsvorfällen.

- Das Erkennen geschieht auf der Ebene von Mitarbeitern oder auch Externen, ggf. auch durch automatische Systeme (Alarmfunktionen, Intrusion Detection).
- Sobald ein vermeintlicher oder tatsächlicher Sicherheitsvorfall erkannt worden ist, muss eine Meldung erfolgen. Dazu muss der Meldeweg dokumentiert sein.

– Läuft eine Meldung beim Sicherheitsmanagement auf, so besteht dessen Aufgabe darin, eine Klassifizierung des Vorfalls vorzunehmen und dann entsprechend dem Ergebnis angemessen zu reagieren. Nähere Informationen zu diesem Thema finden Sie im Abschnitt „14.2 Management von Sicherheitsvorfällen".

Check1 Die Einhaltung des Sicherheitskonzeptes in der Praxis zu garantieren ist eine der Kernaufgaben des Sicherheitsmanagements. Dies verlangt eine entsprechende Überprüfungstätigkeit. Dazu zählen Aktivitäten wie

– Informationsgespräche mit Mitarbeitern führen,
– Vorgaben stichprobenartig auf Einhaltung prüfen,
– technische Untersuchungen (z. B. Penetrationstests) durchführen (lassen),
– Konfigurationen und Einstellungen technischer Systeme überprüfen,
– Checklisten kontrollieren,
– Log-Protokolle prüfen (lassen),
– interne und externe Audits veranlassen.

Dabei sollte es die Regel sein, von allen Aktivitäten dieser Art Aufzeichnungen zu machen. Andernfalls hat das Sicherheitsmanagement kein Material für die Phase *act* und keine objektiven Nachweise für seine Tätigkeiten.

Check2 Eine wichtige Quelle von Informationen sind Sicherheitsvorfälle: Auch wenn ihr Eintreten meist mit einem Schaden verbunden ist, sind sie für das Sicherheitsmanagement geradezu der Paradefall, an dem man erkennen kann, wie es um die reale Sicherheit des Unternehmens und die Praxisnähe seiner Verfahren bestellt ist.

Scherzhaft wird oft gesagt: „Wenn es diesen Vorfall nicht gegeben hätte, hätten wir ihn geradezu herbeiführen müssen…". Sicherheitsvorfälle sind einerseits wichtig, um daraus lernen zu können, andererseits „beflügeln" sie oft Entscheidungen, die vorher nicht zu bekommen waren.

Check3 Jeder IT-Sicherheitsbeauftragte erhält wichtige Informationen durch das Studium von Artikel in Fachzeitschriften bzw. aus dem Internet. Unter Umständen hat man CERT-Dienste abonniert und wird mit „heißen" Meldungen versorgt (s. Abschnitt „5.5 Ergänzendes zur Schwachstellenanalyse"). Solche Informationen sind

dahingehend zu prüfen, ob sie für das eigene Unternehmen relevant sind.

Act1/2

Bei diesen Punkten geht es darum, die Gesamtheit zwischenzeitlich aufgelaufener Informationen auszuwerten, um ggf. Korrektur- und Vorbeugemaßnahmen abzuleiten. Dabei müssen stets mögliche Rückwirkungen auf die Sicherheitsdokumente geprüft werden. Änderungen an der Dokumentation sind zu planen, und zwar in der nächsten Runde mit der Phase *plan*.

Schlussendlich sei angemerkt, dass die Anwendung von PDCA nicht auf die Leitung und das Sicherheitsmanagement beschränkt sein muss. Man kann hierin eine Vorgehensweise für jede am Sicherheitsprozess beteiligte Rolle sehen…

Information Security Forum

Wir haben die Vorgehensweise nach PDCA in einem Organisationsmodell vorgestellt, in dem die *Fachebene* (IT-Sicherheitsmanagement) der *Entscheidungsebene* (Unternehmensleitung) berichtet. In komplexen Unternehmensstrukturen kann es sinnvoll sein, zwischen dem Sicherheitsmanagement und der Leitung ein Entscheidungsgremium einzurichten, in dem die Leitung *und* die Fachebene vertreten sind, um eine Beschlussfähigkeit herzustellen. In den Standards BS 7799 und ISO 17799 wird ein solches Gremium als *Information Security Forum* (ISF) bezeichnet.

2.3 Unverzichtbar: Sensibilisierung, Schulung, Training

Beschäftigen wir uns zunächst mit den Begriffen:

- „Sensibilisieren“ heißt, auf ein für das Unternehmen wichtiges Problem aufmerksam machen.
- „Schulen“ meint, Lösungen für das Problem vermitteln.
- „Training“ hat den Sinn, Lösungen in der Praxis zu üben.

Wir behandeln diese drei Ebenen in den folgenden Abschnitten.

Sensibilisierung

Wer Sicherheit in seinem Unternehmen vorantreiben möchte, macht oft die Erfahrung, dass die Leitungsebene vom Thema IT-Sicherheit nicht gerade begeistert ist. Das geringe Interesse tendiert sogar gegen Null oder provoziert negative Emotionen, wenn man zur Behandlung des Themas Kompetenzen und Ressourcen einfordert. Selbst wenn man die gewünschten Ressourcen nach intensivem Bemühen bekommt, wird man sich immer wieder der Situation ausgesetzt sehen, dass „oben“ kein Verständnis für die Aufgabe der IT-Sicherheit herrscht und man

folglich auch keine Bestätigung oder gar Förderung erwarten darf.

Diese Situation ist grundsätzlich von Übel. IT-Sicherheit lässt sich ohne Mitwirkung und Unterstützung der Unternehmensleitung nicht erreichen. Was hier offensichtlich fehlt, ist eine ausreichende Sensibilität für unser Thema. Wie kann man dem abhelfen?

Als mehr technisch orientierter Mensch denkt man sich, eine überzeugende Argumentationskette müsste es doch bringen: Man betrachtet also

- mögliche Verluste durch unzureichende IT-Sicherheit,
- Anforderungen aus Gesetzen (Stichwort: Risikovorsorge) und Kundenverträgen

und leitet daraus ab, dass IT-Sicherheit notwendig ist. Schafft man es auch noch, potenzielle Verluste durch ein vergleichbar geringes Investment in Sachen IT-Sicherheit abwenden oder reduzieren zu können, ist man am Ziel … glaubt man jedenfalls!

Die Erfahrung zeigt, dass es in hartnäckigen Fällen so nicht geht: Alle Argumente fruchten nichts – aus einem simplen Grund: Es kommt darauf an, *wer* die Argumente vorträgt.

Engagieren Sie einen – vielleicht in letzter Zeit in den Medien sehr präsenten – Sicherheitsexperten und lassen Sie ihn die gleichen Argumente vortragen – plötzlich funktioniert es. Die Psychologie dahinter ist einfach das bekannte Phänomen des „Propheten im eigenen Lande…".

Security Briefing

In diesem Zusammenhang hat es sich bewährt, nicht von Vortrag oder Präsentation zu sprechen, sondern vom „Security Briefing für die Unternehmensleitung". Das Briefing sollte „knackig" und zahlenorientiert präsentiert werden und möglichst mit Beispielen aus der gleichen Branche aufwarten können. Von der Dauer her sollte man maximal 30 Minuten plus Diskussion einplanen. Wichtig ist auch die Nachbereitung: Erstellen Sie ein Protokoll und verbinden Sie die Inhalte mit Vorschlägen zur weiteren Behandlung der IT-Sicherheit im Unternehmen, fügen Sie die Folien des Briefings zur Unterstützung Ihrer Vorschläge bei.

Eine andere bekannte Strategie besteht darin, den ersten schadenträchtigen Sicherheitsvorfall abzuwarten – er kommt bestimmt! –, diesen objektiv mit entsprechenden Zahlen aufzuarbeiten und daran „Vorschläge" zu knüpfen. In diesem Moment sind Management-Entscheidungen und Ressourcen oft sehr viel leichter zu bekommen.

Fehlende Sensibilität ist natürlich nicht nur ein Thema für die Leitungsebene. Auch unter den Mitarbeitern trifft man oft auf die Situation, dass Personen mit „Sicherheit“ nicht viel anfangen können, sich bei ihrer Arbeit gestört oder behindert fühlen, vielleicht sogar einen besonderen Reiz daran finden, bestehende Sicherheitsvorkehrungen bewusst zu unterlaufen. Auch hier gilt es, die Sensibilität zu erhöhen. Man sollte dies auf drei Ebenen angehen, nämlich

- regelmäßig (z. B. monatlich) interessante Sicherheitsinformationen bereit stellen,
- regelmäßig (z. B. ein- bis zweimal jährlich) eine interessante interne Veranstaltung zum Thema IT-Sicherheit durchführen, dabei z. B. über reale Schadenvorfälle berichten und ihre Auswirkungen auf das Unternehmen darstellen, vielleicht einen professionellen Hacker für eine Live-Demo einladen,
- in hartnäckigen Fällen Mitarbeiter persönlich ansprechen und Überzeugungsarbeit leisten.

Eine wichtige grundsätzliche Erkenntnis in Sachen Sensibilisierung ist, dass sie periodisch aufgefrischt werden muss.

Schulung

Sobald eine Sicherheitsleitlinie vorliegt und spätestens, wenn ein Sicherheitskonzept erstellt worden ist, geht es darum, die Inhalte geeignet an die Mitarbeiter zu vermitteln. Grundsätzliches Ziel der Schulung ist es, das notwendige Sicherheitswissen zu vermitteln, und zwar bezogen auf den jeweiligen Arbeitsplatz und dessen Anforderungen. Jeder Mitarbeiter muss deshalb die Sicherheitsziele und Sicherheitsmaßnahmen kennen, die für seinen Arbeitsplatz und die von ihm bekleideten Rollen wichtig sind.

- Je nach Thema kann man Schulungsmaßnahmen extern beauftragen oder selbst durchführen.
- Manche Unternehmen verwenden Computer-Based-Training (CBT), um die Schulungsinhalte durch die Betroffenen selbst erarbeiten zu lassen. Aber auch klassische Frontal-Schulungen sollte man nicht ausschließen.

– Personen mit sicherheitskritischen Aufgaben wie z. B. System- und Firewall-Administratoren, Operator und Backup-Verantwortliche brauchen weitergehende Schulungen, und zwar zu den Systemen und Produkten, die sie bei ihren sicherheitskritischen Tätigkeiten nutzen. Solche Schulungen werden durch die Hersteller der Systeme oder durch einschlägige Schulungsveranstalter angeboten.

Ein Bedarf an *neuen* Schulungsmaßnahmen ergibt sich stets bei Systemwechsel oder kritischen Änderungen, beim Einsatz neuer IT-Produkte und -Anwendungen, bei gravierenden Änderungen an den Sicherheitszielen und -maßnahmen.

Training

Für sicherheitskritische Rollen reichen Sensibilisierung und Schulung nicht aus: Hier geht es zusätzlich darum, die sicherheitskritischen Tätigkeiten durch wiederholtes Üben so im Bewusstsein zu verankern, dass die kritischen Arbeitsvorgänge im Bedarfsfall routiniert und fehlerfrei ausgeführt werden können.

Regelmäßige Übungen der Feuerwehr finden nicht etwa statt, um das Verfahren der Löschung von Bränden kennen zu lernen, sondern um im Brandfall aus dem Unterbewusstsein heraus genau das Richtige zu tun. Das gleiche Ziel verfolgen wir im Grunde auch bei der IT-Sicherheit. In unserem Kontext betrifft die Notwendigkeit von Training jede Art von Notfallbehandlung wie z. B. bei Virenbefall, beim Einbruch durch Hacker, beim Versagen kritischer Systeme, bei Backup und Recovery, beim Umschalten auf Ausweichrechenzentren und beim Zurückschalten.

Planung

Bei der Vielzahl von Aspekten zu diesem wichtigen Thema muss eine gute Planung dringend angeraten werden. Am besten wird jedes Jahr ein Plan aufgestellt, in dem alle vorgesehenen Maßnahmen zu diesem Themenkomplex erfasst und vom Aufwand her beziffert sind.

Nachweise

Wichtig ist auch die Nachweisführung über umgesetzte Maßnahmen. Hierzu zählen Schulungsnachweise, Teilnehmerlisten von internen Veranstaltungen, Archivieren von bereit gestellten Sicherheitsinformationen, Aufzeichnungen über Trainingsmaßnahmen einschließlich entsprechender Auswertungen.

Zum Abschluss: Manche Sicherheitsexperten sagen, dass die beschriebenen personellen Maßnahmen bereits 50% der IT-Sicherheit bringen…

2.4 Management der Dokumentation

Im Laufe des Sicherheitsprozesses entstehen viele Dokumente wie z. B.

- die Sicherheitsleitlinie,
- das Sicherheitskonzept oder dem entsprechende Dokumente gemäß ISO 27001 oder IT-Grundschutz,
- spezielle Sicherheitsrichtlinien zu wichtigen Themen für bestimmte Gruppen (meist Extrakte aus dem Sicherheitskonzept in anderer Formulierung),
- Verfahrensbeschreibungen zu Geschäftsprozessen (zusammenfassende Darstellung der Abläufe, der verwendeten Technik und der beteiligten Rollen),
- Arbeitsanweisungen mit Checklisten – zumindest für alle sicherheitsrelevanten Rollen,
- Inventarverzeichnisse (Räume, IT-Systeme, Netzwerkkomponenten, physische Sicherheitseinrichtungen, Verkabelungspläne, betriebene Anwendungen bzw. Geschäftsprozesse),
- Handbücher für IT- und sonstige Systeme,
- Berichte zur Sicherheitslage bzw. über Sicherheitsvorkommnisse, Protokolle von Besprechungen / Aufzeichnungen, Nachweise.

Umso wichtiger ist es, von vorneherein eine tragfähige Struktur aufzubauen, um den Überblick behalten und auch die Auswirkungen von Änderungen leichter analysieren zu können.

Als sehr nützlich hat sich die Vorstellung von einer *Dokumentenpyramide* erwiesen, die jeweils von oben nach unten

- die Hierarchie der Dokumente visualisiert (vom Allgemeinen zum Speziellen),
- ihre Änderungshäufigkeit charakterisiert (eher stabil bis häufig zu ändern).

Abbildung 2: Dokumentenpyramide

Berechtigungen

Manche Dokumente werden für *alle* Mitarbeiter des Unternehmens zugänglich sein müssen – etwa die Sicherheitsleitlinie und manche Sicherheitsrichtlinien. Andere Unterlagen werden nur im Kreis der für die Sicherheit unmittelbar Verantwortlichen bleiben (etwa das Sicherheitskonzept). Möglicherweise gibt es auch Unterlagen (z. B. einzelne Berichte), die nur für die Unternehmensleitung gedacht sind.

Vor diesem Hintergrund ist klar, dass man eine *Klassifizierung* der Dokumente nach Adressatenkreis bzw. Verteiler vornehmen muss:

- Stellen Sie sicher, dass jeder Adressatenkreis über die für ihn wichtigen Dokumente, und zwar in der jeweils aktuellen Fassung, verfügt.
- Stellen Sie sicher, dass andere Personen, die nicht zum Adressatenkreis gehören, keinen Zugriff auf das entsprechende Dokument haben.

Das klassische Vorgehen besteht darin, das jeweilige Dokument zu drucken und an die Adressaten auszuhändigen – wobei dann ältere Fassungen manuell aus dem Verkehr gezogen werden müssen.

Die modernere Lösung besteht in der Nutzung des Intranets des Unternehmens: Hier könnten die aktuellen Sicherheitsdokumente auf einer entsprechende Web-Seite zur Verfügung gestellt werden. Dabei muss aber das Problem der unterschiedlichen Zugriffsrechte je nach Adressatenkreis gelöst werden. Darüber hinaus ist zu bedenken, dass bei einem Sicherheitsvorfall die Verfügbarkeit der Web-Seite oder des gesamten Intranets nicht mehr gegeben sein kann. In einem solchen Fall stehen wichtige Sicherheitsinformationen nicht mehr zur Verfügung.

Vor diesem Hintergrund kommt man in der Praxis meist zu einer „gemischten" Vorgehensweise, bei der die für Notfälle wichtigen Informationen klassisch in Papierform übermittelt werden, während das Intranet für alle anderen Unterlagen genutzt wird.

Listen

Für die Erstellung und Weiterentwicklung sowie den Umgang mit Sicherheitsdokumenten gelten folgende Empfehlungen:

- Führen und pflegen Sie eine zentrale Liste aller gültigen Sicherheitsdokumente mit Angabe des Versionsstandes und des Ausgabedatums. Die Liste selbst kennzeichnen sie mit einem Datum.
- Führen und pflegen Sie eine zentrale Liste sonstiger Dokumente, die Sie verwenden oder verwendet haben, wie z. B. Standards, Gesetze und Verordnungen, Maßnahmen-Kataloge, Internet-Links. Die Liste selbst kennzeichnen Sie mit einem Datum.

Verweisen Sie in allen anderen Dokumenten auf diese Listen mit dem Zusatz „aktuelle Fassung": Verwenden Sie hierfür und für die Referenz auf Dokumente aus diesen Listen keine Versions- und Datumsangaben – sonst müssen Sie bei jeder Änderung irgendeiner Version oder irgendeines Datums alle Dokumente aktualisieren!

Dokumentvorlagen

Nutzen Sie einheitliche Dokumentvorlagen für alle anfallenden Dokumente. Bereiten Sie die Vorlagen so vor, dass auf dem Titelblatt folgende Angaben verlangt werden:

- Titel und ggf. Untertitel,
- Kennzeichnung als Entwurf oder als in Kraft gesetztes Dokument,
- Adressatenkreis: Wer soll bzw. darf das Dokument lesen?,
- Angaben zum aktuellen Stand des Dokumentes (Version und Datum),

– Autoren des Dokumentes,
– Prüf- und Freigabevermerke: Name des Freigebenden, Datum der Freigabe.

Das Dokument sollte auf einer der weiteren Seiten eine Dokumentenhistorie enthalten, in der festgehalten wird, weshalb die Vorläufer und die aktuelle Fassung jeweils herausgegeben wurden.

Glossar

In den vorausgehenden Abschnitten ist schon mehrfach darauf hingewiesen worden, dass klare Begrifflichkeiten für den Sicherheitsprozess unerlässlich sind. Erstellen Sie am besten gleich zu Beginn ein Glossar, stimmen es unter den Beteiligten ab und legen Sie es für die folgenden Arbeitsschritte als verbindlich zugrunde. In allen anderen Sicherheitsdokumenten verweisen Sie auf dieses Glossar mit dem Hinweis „aktuelle Fassung". Den Stand des Glossars kennzeichnen sie mit einem Datum.

Sie können das Glossar auch in einzelne Dokumente per Feldfunktion einbinden, um später per Knopfdruck Aktualisierungen durchführen zu können. Wenn Sie dies tun: Ein Glossar gehört an den *Anfang* eines Dokumentes – steht es am Ende, wird es meist übersehen und verfehlt seinen Zweck.

Als Ausgangspunkt für ein Glossar können die Begriffe aus dem Kapitel „3. Grundstrukturen der IT-Sicherheit" dienen.

ISO 900x

Falls im Unternehmen ein Qualitätsmanagement etwa gemäß ISO 900x eingerichtet ist, kann es sein, dass die zuvor beschriebenen Empfehlungen längst umgesetzt worden sind und nur noch für die Zwecke der IT-Sicherheit adaptiert bzw. übernommen werden müssen.

Bei dieser Gelegenheit: Es könnte generell von Nutzen sein, die IT-Sicherheit als einen QM-Prozess in das Qualitätsmanagement einzuordnen…

3 Grundstrukturen der IT-Sicherheit

In den folgenden Abschnitten wollen wir wichtige begriffliche Grundlagen bereitstellen und im Zusammenhang erläutern. Gleichzeitig werden wir eine Reihe von Ideen und Konzepten aufarbeiten, die sich als Bausteine für ein Vorgehensmodell eignen. Dabei streben wir eine „ganzheitliche" Sicht an, d. h. wir hängen die Sicherheit sehr hoch auf, und zwar letztlich an den Geschäftsprozessen von Unternehmen[3], und betrachten dabei nicht nur die unterstützende IT sondern das gesamte Umfeld.

Wie (Informations-, Daten-, IT- oder System-) *Sicherheit* zu definieren ist, werden wir in den folgenden Abschnitten erarbeiten. Besonderen Wert legen wir von Anfang an auf eine strukturierte Dokumentation. Ihr Fehlen ist nach einhelliger Meinung eines der großen Defizite in der IT-Sicherheit: Sicherheit beginnt mit einer „sicheren", d. h. die Realität nachvollziehbar und korrekt beschreibenden Dokumentation. Erst mit einer aussagekräftigen und gut strukturierten Dokumentation ist man in der Lage, Analysen der Sicherheit durchzuführen und eine *reale* Einschätzung der eigenen Sicherheit zu bekommen.

Zwei zentrale Dokumente sind zu nennen, nämlich

- die Sicherheitsleitlinie[4], in der die Frage „warum brauchen wir IT-Sicherheit in unserem Unternehmen" behandelt wird, und
- das Sicherheitskonzept, in dem die Frage „wie viel Sicherheit brauchen wir und wie erreichen wir sie" minutiös beantwortet werden soll.

Wir werden auf diese beiden Dokumente noch sehr viel detaillierter eingehen.

---

3 bzw. den Verwaltungsverfahren von Behörden

4 auch „Security Policy" und (fälschlicherweise) „Sicherheitspolitik" genannt

3.1 Organisation und Personal

Rollen

Als *Rolle* bezeichnen wir eine Funktion in einem Unternehmen, der Rechte und Pflichten zur Erfüllung bestimmter Aufgaben zugewiesen sind. Eine Rolle kann in der Praxis durch *eine* Person oder auch durch *mehrere* Personen ausgefüllt werden. Typischerweise hat jeder Rolleninhaber eine Vertretung, so dass wir meist zumindest zwei Personen als Besetzung für eine Rolle haben.

Rollen- und Besetzungsliste

Sinnvollerweise legt man sich eine Liste der Funktionen bzw. Rollen des Unternehmens an – zumindest soweit diese für das Sicherheitsthema wesentlich sind. Dazu zählen natürlich der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement, der Datenschutzbeauftragte, System-Administratoren und Operator, Beauftragte für die Infrastruktur, der Werkschutz, die Personalvertretung, usw.

Es wäre wünschenswert, für jede Rolle auf dieser Liste eine Rollenbeschreibung zur Verfügung zu haben, in der folgende Informationen enthalten sind:

- eine Übersicht über die der Rolle zugewiesenen Aufgaben und Verantwortlichkeiten,
- Verweise auf Arbeitsanweisungen und Checklisten für die jeweilige Rolle (sofern notwendig),
- die aktuellen Namen und Kontaktdaten der Rolleninhaber.

Rollenausschlüsse

Es kann Rollen geben, die miteinander unverträglich sind, d. h. sie sollten bzw. dürfen nicht von der gleichen Person besetzt sein. Ein typisches Beispiel sind die beiden Rollen RZ-Leiter und IT-Sicherheitsbeauftragter: Hier ist aus Gründen des Interessenkonfliktes ein Rollenausschluss vorzusehen.

In der Praxis erstellt man sich eine Matrix, die die festgelegten Rollen in Zeilen und Spalten enthält; dann markiert man in den Kreuzungspunkten die Rollenausschlüsse oder trägt bestimmte Bedingungen für die Rollenverträglichkeit ein.

Arbeitsanweisungen

Für jede Rolle, die sicherheitsrelevante Tätigkeiten übernimmt, sollte eine entsprechende Arbeitsanweisung vorliegen, in der die Aufgaben Schritt für Schritt zumindest soweit präzisiert sind, dass eine korrekte und nachvollziehbare Abwicklung der Tätigkeiten gewährleistet ist. Jede Arbeitsanweisung wird ggf. weitere Rollen aufführen, die bei den Tätigkeiten zu beteiligen sind, und die entsprechenden Schnittstellen erläutern.

Checklisten Bei besonders sicherheitskritischen Tätigkeiten sieht man ergänzend eine Checkliste vor, die bei jeder Durchführung von Arbeiten ausgefüllt und unterschrieben wird. Solche Nachweise sind z. B. bei der Installation und Konfiguration von IT-Systemen, Administrationsarbeiten, Update-Prozessen, dem Backup und Recovery notwendig; besonders prädestiniert sind auch Tätigkeiten an sensitiven Systemen wie z. B. die Konfiguration von Firewalls.

Besetzungsliste Es ist sinnvoll, im Rollenverzeichnis in einer weiteren Spalte die aktuellen Namen der Rolleninhaber und Vertreter („Besetzungsliste“) einzutragen und diese Eintragungen entsprechend zu pflegen.

Qualifikation Zumindest bei Rollen, die sicherheitsrelevante Aufgaben haben, sollte festgelegt werden,

- welche Anforderungen an Ausbildung, Berufserfahrung und Spezialkenntnisse erforderlich sind (Anforderungsprofil),
- wie diese Qualifikationen aufrechterhalten bzw. weiterentwickelt werden sollen.

Solche Informationen sind insbesondere für die *Besetzung* von Rollen und die Ressourcenplanung wichtig.

Zur Erstellung und Pflege des Rollenverzeichnisses und der Rollenbeschreibungen haben wir in der Abbildung 3 die Funktionen „Manager-1“ und „Manager-2“ (letzterer für jede Rolle separat) eingetragen.

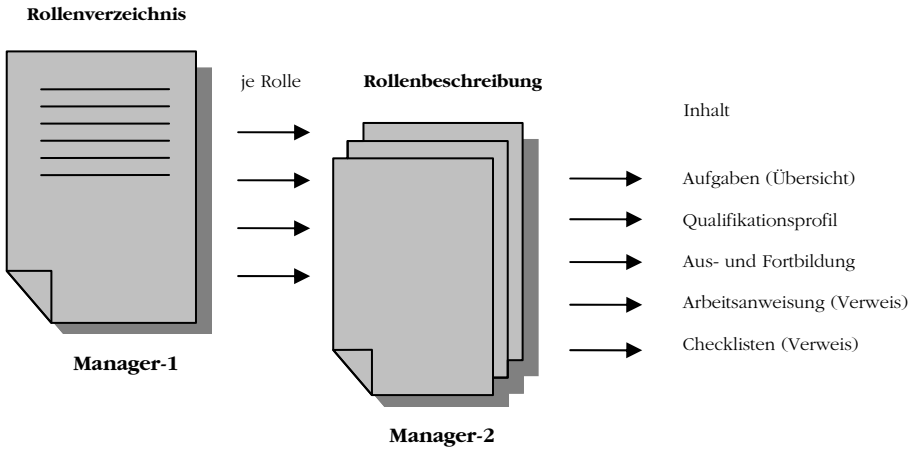

Abbildung 3: Dokumentation zu Rollen

Bei den Arbeitsanweisungen und Checklisten ist ebenfalls festzulegen, wer für deren Erstellung und Pflege zuständig ist.

Organisation

Immer wieder wird die Frage gestellt, wie die Sicherheit im Unternehmen zu organisieren ist. Soll es eine eigene Sicherheitsabteilung geben? Vielleicht ein Querschnitts-Gremium oder ein Sicherheitsforum? Oder ist die Sicherheitsthematik nur einer bestimmten Person zugewiesen?

Zunächst ist festzuhalten, dass die IT-Sicherheit ein Element der Unternehmensvorsorge ist und damit als Aufgabe bei der Unternehmensleitung liegt. Diese wird die Verantwortung vor allem nach außen wahrnehmen, intern aber eine Zuständigkeit für dieses Thema definieren – das (IT-)Sicherheitsmanagement. Diese Zuständigkeit wird in der Praxis entweder durch eine Person plus Vertreter, eine Stabsabteilung oder durch ein Gremium realisiert – letzteres mit Vertretern aus solchen Organisationseinheiten, die Beiträge zur Sicherheit leisten können und müssen.

Gleich welche Organisationsform gewählt wird – wir sprechen im Folgenden immer vom „(IT-)Sicherheitsmanagement“ als Organisationsbezeichnung und von der Rolle "(IT-)Sicherheitsbeauftragter".

Einordnung des IT-Sicherheitsbeauftragten

Wie ist nun diese Rolle einzuordnen? Besteht die Aufgabe darin, die Unternehmensleitung in Sachen IT-Sicherheit zu *beraten*? Oder ist der IT-Sicherheitsbeauftragte intern *verantwortlich* für die IT-Sicherheit des Unternehmens?

Die Praxis zeigt, dass alle Formen vorkommen – von einer reinen Beratungsfunktion (vielfach z. B. bei Behörden) bis hin zur vollen Übernahme der Verantwortung (häufig in straff organisierten Unternehmen). Die Übernahme der Verantwortung kann soweit gehen, dass die IT-Sicherheit in Zielvereinbarungen auftaucht und Auswirkungen auf das Gehalt hat. Konsequenzen bei "schlechtem" Management – was das auch immer heißen mag und wie es gemessen wird – sind dann ähnlich wie bei Umsatzverantwortlichen mit einem zu geringen Jahresumsatz. Grundsätzlich sollte die Funktion natürlich so angelegt sein, dass mehr Verantwortung auch mehr Entscheidungsfreiheit bedeutet.

Es wird dringend angeraten, in einer Rollenbeschreibung schriftlich festzuhalten,

- wer für das Thema IT-Sicherheit zuständig ist: Person, Gremium, Abteilung,
- was mit der Zuständigkeit gemeint ist: Beratung bzw. Grad der Verantwortung,

- wie weit die Zuständigkeit inhaltlich reicht: z. B. zuständig nur für einen Teil der IT oder für einige benannte Geschäftsprozesse,
- welche Ziele (zeitlich, inhaltlich) gesetzt sind,
- womit diese Ziele erreicht werden sollen: Entscheidungsbefugnisse, Ressourcen.

Es ist anerkannte Praxis und auch in Standards niedergelegt, dass die Rolle "IT-Sicherheitsbeauftragter" direkt der Unternehmensleitung unterstellt ist und dieser berichtet. Gegebenenfalls sollte sie einem breiter angelegten Sicherheitsmanagement vorstehen.

Bereits erwähnt wurde, dass die Funktion "IT-Sicherheitsbeauftragter" nicht vereinbar ist mit der operativen Leitung beispielsweise des Rechenzentrums oder der Verwaltung, weil hierbei in der Praxis sehr schnell Interessenkonflikte – meist zum Nachteil der IT-Sicherheit – auftreten werden. Deshalb ist diese Aufgabe von anderen operativen Tätigkeiten zu trennen. Ein Problem ist dies bei kleineren Unternehmen, in denen die Funktion des IT-Sicherheitsbeauftragten oft eine Teilzeit-Funktion ist; hier erhält dann *eine* Person schnell mehrere unverträgliche Rollen zugewiesen.

Grundsätzlich sollte der IT-Sicherheitsbeauftragte weisungsfrei gestellt werden, d. h. er untersteht nicht Weisungen anderer Fach-Abteilungen – natürlich aber den Weisungen der Unternehmensleitung. Aber auch bei letzterem muss geklärt sein, dass der IT-Sicherheitsbeauftragte seine fachlichen Ansichten unabhängig präsentieren kann; die Entscheidung über seine Vorschläge liegt aber letztlich bei der Leitung.

Arbeitsgruppe

Auch wenn die Funktion des IT-Sicherheitsbeauftragten einer einzelnen Person zugewiesen worden ist, sollte diese eine spezielle Arbeitsgruppe zur IT-Sicherheit („Koordinierungsgremium“) einrichten, in der zumindest die zur IT-Sicherheit beitragenden Rollen vertreten sind: Datenschutzbeauftragter, Vertreter der Fachabteilungen einschließlich der Verwaltung und die Verantwortlichen für einzelne Geschäftsprozesse, Vertreter des Rechenzentrums bzw. der IT-Abteilung. Möglicherweise wird diese Arbeitsgruppe sogar in Form des ISF (s. Ende des Abschnitts 2.2) eingerichtet.

Aufgaben des IT-Sicherheitsbeauftragten

Kehren wir zur Ausgangsfrage nach den Aufgaben des IT-Sicherheitsbeauftragten zurück und beantworten wir diese zunächst für ein in sich geschlossenes Unternehmen mit *einem* IT-Sicherheitsbeauftragten:

- In Abstimmung mit und nach Vorgaben der Leitung ist ggf. die Sicherheitsleitlinie des Unternehmens zu erstellen, die anschließend von der Leitung in Kraft zu setzen ist (vgl. Kapitel „6. Die Sicherheitsleitlinie“).
- Aus der Sicherheitsleitlinie sind das Sicherheitskonzept und alle dazu gehörenden Begleitdokumente zu entwickeln, im Unternehmen abzustimmen und der Umsetzung zuzuführen (vgl. Kapitel „8. Das Sicherheitskonzept“).
- Der Themenbereich „Sensibilisierung, Schulung, Training“ ist zu planen und umzusetzen (vgl. Abschnitt 2.3).
- Ein zentrales Sicherheits-Informationssystem ist einzurichten und aktuell zu halten.
- Die korrekte Einhaltung des Sicherheitskonzeptes ist kontinuierlich zu prüfen (vgl. Abschnitt „14.1 Aufrechterhaltung der Sicherheit“).
- Sicherheitsvorfälle müssen geeignet behandelt werden (vgl. Abschnitt „14.2 Management von Sicherheitsvorfällen“).
- Es ist ein Berichtswesen aufzubauen und zu betreiben, darin eingeschlossen die Verfahren zur Generierung von Nachweisen (vgl. Abschnitt „14.3 Berichtswesen“).
- Eine Wartung aller Sicherheitselemente – Dokumentation, Maßnahmen, Prozesse – ist zu planen und durchzuführen (vgl. Abschnitt „2.2 Das PDCA-Modell“).

Konzerne

Etwas anders sieht es bei größeren Konzernen aus: In den einzelnen Gesellschaften des Konzerns wird es eigene IT-Sicherheitsbeauftragte geben, die die zuvor beschriebenen Aufgaben auszuführen haben. In der oberen Konzernebene (Holding etc.) wird ein „zentraler IT-Sicherheitsbeauftragter“ anzusiedeln sein, dessen Aufgaben insbesondere darin bestehen,

- die Sicherheitsleitlinie des Konzerns aktuell und verbindlich zu halten,
- gewisse Vorgaben zur Interoperabilität bei der Sicherheit zwischen den Konzerntöchtern herzustellen (z. B. Vorgaben über einheitlich anzuwendende Verschlüsselungsverfahren),
- ein zentrales Sicherheits-Informationssystem für den Konzern einzurichten und zu betreiben,
- ggf. das Thema „Sensibilisierung, Schulung, Training“ übergreifend zu organisieren,

– sich von den IT-Sicherheitsbeauftragten der einzelnen Konzerntöchter die Einhaltung der Sicherheitsleitlinie regelmäßig nachweisen zu lassen.

Darüber hinaus wird er ggf. für die Sicherheit der Holding selbst zuständig sein.

Die IT-Sicherheitsbeauftragten der Konzerngesellschaften werden ihrerseits die „von oben" kommende Sicherheitsleitlinie durch ein Sicherheitskonzept konkretisieren, dieses umsetzen und dabei Nachweise generieren, die zeigen, dass die Konzern-Sicherheitsleitlinie korrekt umgesetzt wurde.

Besitzt der Konzern mehr als nur die zwei beschriebenen Ebenen (Holding und Tochtergesellschaften), so wird dies so zu organisieren sein, dass stets die von einer Ebene kommenden Vorgaben zur IT-Sicherheit

– durch die nächst tiefere Ebene umgesetzt und
– entsprechende Nachweise „nach oben" weitergegeben werden.

Mit diesem Schema hat jeder IT-Sicherheitsbeauftragte

– Vorgaben zu erlassen bzw. von höheren Ebenen weiterzugeben und
– die Einhaltung der Vorgaben in seinem Bereich zu überwachen.

Genau hiermit kommt er seiner Manager-Pflicht nach. Leider zeigen einschlägige Untersuchungen, dass der letzte Punkt meist sträflich vernachlässigt wird – selbst dort, wo ansonsten von der Vorgabenseite her alles in Ordnung ist. Die Statistiken weisen für Deutschland einen Anteil von weniger als 15% derjenigen Unternehmen aus, die die Einhaltung ihrer Vorgaben auch umfassend prüfen.

3.2 Information und Daten

Es klingt banal, aber an einer klaren Unterscheidung zwischen den Begriffen *Information* und *Daten* hängt schon ein wesentlicher Beitrag zur ganzheitlichen Sicherheit.

Information, Daten

Mit *Information* meinen wir immer den Informationsgehalt, d. h. den Inhalt einer Nachricht, einer Datei oder eines Dokumentes. Jede Darstellung bzw. Wiedergabe dieser Information in codierter Form bezeichnen wir als *Daten*.

Eine Codierung in diesem Sinne ist beispielsweise die Wiedergabe einer Information in gedruckter Form, als magnetische oder optisch lesbare Aufzeichnung auf Datenträgern, in elektrischen oder optischen Signalen z. B. bei der Datenübertragung, bei der Anzeige auf einem Bildschirm.

Eine andere Art von „Codierung“ begegnet uns im Zusammenhang mit der Verschlüsselung: Daten werden so verschlüsselt, dass die Rückgewinnung der Information von der Kenntnis eines geheimen Schlüssels und eines Verschlüsselungsverfahrens abhängig ist.

Eine weitere Variante: Informationen werden in nichtssagenden, aber lesbaren Kürzeln, Codewörtern oder ganzen Sätzen versteckt, so dass Personen ohne Kenntnis des Kontextes die Information nicht oder nur schwer zurückgewinnen können.

Ganz besonderen Informationen und Daten begegnen wir im folgenden Fall:

Programme, Software

Ein *Programm* ist eine abstrakte Information über einen vorgesehenen Verfahrensablauf. Darstellungen eines Programms in Form von Ablaufdiagrammen, Quellcode und Object Code sind damit *Daten* in unserem Sinne; Quell- und Object Code bezeichnen wir dabei als *Software*.

Datenstrukturen

Daten sind meist in Strukturen eingebettet: Sie können in Dateien, Sätzen und Feldern einer Datenbank, in Datenpaketen bei der Kommunikation, in Betriebssystem-internen Strukturen wie Puffern und Warteschlangen und auf Datenträgern in Blöcken usw. organisiert und gespeichert sein – aber natürlich auch seitenweise auf Papier ausgedruckt und sodann in Ordnern abgeheftet worden sein. Eine kurze Zusammenfassung anhand von Beispielen liefert die folgende Tabelle:

Tabelle 3: Daten und Datenstrukturen

Kontext	Information	Daten	Datenstruktur
Nachrichtenaustausch	Nachrichteninhalt	Darstellung der Nachricht in ASCII-Zeichen	Email
Software-Anwendung	Programmablauf	Darstellung des Programms in Maschinencode	Exe-Datei

Kontext	Information	Daten	Datenstruktur
Kunden-verwaltung	Kundenname	Kundenname in ASCII-Zeichen	Feld einer Datenbank
Schriftwechsel	Kunden-mitteilung	Ausdruck in normaler Schrift	Blätter / Seiten in Akten

Warum nun der Unterschied zwischen Informationen und Daten? Fokussiert man nur auf die elektronisch gespeicherten Unternehmensdaten, dann läuft man Gefahr, hierfür umfangreiche und teure Sicherheitsmaßnahmen vorzusehen, während die zu schützenden Informationen leicht

- von Personen in unbefugter Weise z. B. in Gesprächen auf Dienstreisen weitergeben werden,
- in externen Systemen – etwa private IT-Systeme – gespeichert und "verarbeitet" werden,
- in Papierform ungeschützt herumliegen.

Die Investition in Sicherheitsmaßnahmen ausschließlich für die IT des Unternehmens ist dann nur von beschränktem Nutzen. Macht man sich dagegen klar, wo überall die zu schützenden Informationen tatsächlich vorhanden sind und schließt daran Sicherheitsrichtlinien und -maßnahmen an, hat man einen ersten Schritt zu einem *ganzheitlichen* Konzept des Informationsschutzes getan. Es sind in unserem Beispiel insbesondere Regelungen über Gespräche vertraulichen Inhalts mit Externen bzw. Unbefugten, die Mitnahme von Daten außerhalb des Unternehmens, den Umgang mit dem Datenträger Papier zu treffen.

3.3 Datenträger und Datenverarbeitung

Daten in dem zuvor beschriebenen Sinne benötigen immer ein Trägermedium. Während die historischen Datenträger Lochstreifen und Lochkarten nur noch in Ausnahmefällen Verwendung finden, haben wir es heute mit Papier (für Ausdrucke), Disketten, CD und DVD, Magnetbändern und Kassetten zu tun – aber auch mit USB-Sticks, (eingebauten oder mobilen) Festplatten, optische Datenträger und natürlich mit Speichern in Form von Arbeitsspeicher, temporär genutzte Speicher in Tastaturen, Laufwerken. Für den Datentransfer genutzte Leitungen und andere

Übertragungsstrecken (z. B. per Funk) sind ebenfalls hier einzuordnen.

Wichtig ist, sich eine Liste der im Unternehmen verwendeten Datenträger zu erstellen und hierauf aufbauend zu überlegen, ob für den Umgang mit bestimmten Datenträgern Regelungen zu treffen sind.

Typische Beispiele hierfür sind Regelungen

- zum Umgang mit Disketten und CD/DVD (betreffend Mitnahme aus dem Unternehmen bzw. Hereinbringen von Fremd-Datenträgern),
- zur Klassifizierung von Netzwerkstrecken (basierend auf der Sensitivität der übertragenen Daten)
- zur Reparatur und Außerbetriebnahme von Festplatten (mit sensitivem Inhalt).

Datenverarbeitung

Unter *Verarbeitung* von Daten fällt alles, was man mit Daten tun kann, insbesondere

- die Eingabe von Daten in ein technisches System per Tastatur, Scanner, etc.,
- die Speicherung in Datenstrukturen bzw. Dateien,
- die Verknüpfung und Auswertung von Daten z. B. durch Programme,
- die Anzeige und die Ausgabe von Ergebnissen (z. B. Ausdruck),
- die Übertragung von Daten,
- das Löschen von Daten,
- die Vernichtung von Daten(trägern),
- das Duplizieren von Daten(trägern),
- das Ausführen eines Programms (Object Code als Daten).

Eine Verarbeitung von Daten findet auch statt, um komplexe Vorgänge zu überwachen und zu steuern: „Messen – Steuern – Regeln“.

3.4 IT-Systeme und Einsatzumgebung

IT-System

Als *IT-System* bezeichnen wir jedes technische System, das Daten in einer der zuvor beschriebenen Formen automatisiert verarbeiten kann.

Einige Beispiele: Zu den IT-Systemen zählen wir

- Rechner wie PC, Workstations, Mainframes,
- Spezialsysteme wie Gateways, Router und Firewalls,
- Systeme zum Messen, Steuern, Regeln,
- aber auch heute meist „intelligente“ Systeme wie Drucker, Bildschirme, Scanner, TK-Anlagen, Speichersubsysteme und Archivsysteme.

In unsere ganzheitliche Betrachtungsweise müssen wir auch

- Aktenschränke: „Speichern“ von gedruckten Daten,
- Datentresore: Aufbewahren von Sicherungsdatenträgern,
- Aktenvernichter: Vernichten von gedruckten Daten und
- Kopiergeräte: Duplizieren von gedruckten Daten

einbeziehen.

Bei allen IT-Systemen wollen wir Firmware und Betriebssystem sowie weitere Betriebssystem-nahe Software stets als zum IT-System gehörig betrachten.

IT-Inventar-verzeichnis

Es führt kein Weg daran vorbei: Erfassen Sie die IT-Systeme des Unternehmens in einem zentralen IT-Inventarverzeichnis. Diese Liste muss die einzelnen Systeme aufführen, ihren *Standort* benennen, eine grobe Angabe des *Verwendungszwecks* sowie einen Verweis auf die spezifische *System-Dokumentation* beinhalten, sofern eine solche vorhanden ist.

System-Dokumentation

Als Bestandteil dieser System-Dokumentation sehen Sie folgende Informationen vor (für das Beispiel klassischer IT):

- Angaben über die Hardware-Ausstattung,
- Angaben zur Firmware, zum Betriebssystem und zur Betriebssystem-nahen Software,
- Konfigurationsvorgaben und -daten,
- die für Installation, Administration, Betrieb und Wartung, ggf. auch Vernichtung zuständige Personen,
- Verweise auf die Hersteller-Manuale für die Benutzer und System-Administratoren,
- einzuhaltende Umgebungsbedingungen wie z. B. Klimadaten, Belastung von Versorgungsleitungen, zulässige Deckenlasten,

– div. Aufzeichnungen über die Inbetriebnahme, Log-Versuche, Fehler- und Störungsfälle, Wartung und Außerbetriebnahme.

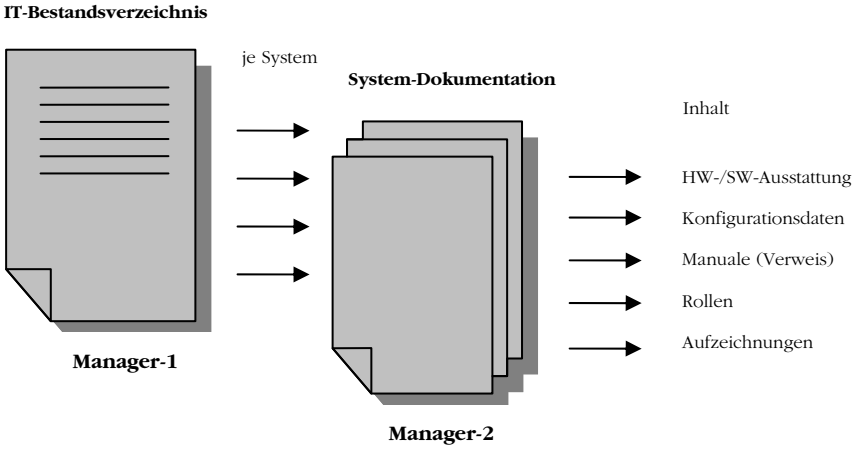

Abbildung 4: Dokumentation zum IT-Bestand

Das IT-Inventarverzeichnis und die System-Dokumentationen sind zu erstellen und zu pflegen; dafür benötigen wir zuständige Rollen[5] – in der Abbildung 4 als „Manager-1“ und als „Manager-2“ bezeichnet, „Manager-2“ wird dabei ggf. von System zu System eine andere Rolle sein. Diese Rollen müssen festgelegt und mit Personen besetzt werden.

3.5 Infrastruktur

Jedes IT-System ist eingebettet in eine physische Infrastruktur: Hierzu rechnen wir

– die für das IT-System genutzten Räumlichkeiten mit ihren begrenzenden Decken und Mauern, Fenstern und Türen,

– die technischen Schnittstellen der Räumlichkeiten nach außen wie z. B. Versorgungsleitungen und Netzwerkverkabelung,

---

5 Wir verwenden wiederum die Zusätze „-1“ und „-2“; dennoch handelt es sich natürlich nicht um die gleichen Funktionen wie in der Abbildung 3. Analog gilt das für die im Weiteren noch aufgeführten Funktionen.

– die nicht direkt IT-bezogene Ausstattung der Räumlichkeiten wie z. B. Feuermelder und Löscheinrichtungen, andere Melde- und Warnsysteme, Zutrittskontrolleinrichtungen.

Manuelle Verarbeitungen mit Daten wie das Kopieren, Abheften, Weitergeben, Vernichten per Reißwolf, Unterzeichnen usw. sind in unserem ganzheitlichen Verständnis von Informationsschutz ebenfalls zu betrachten und finden in Büroräumen statt. In aller Regel haben *Büroräume* heutzutage eine IT-Ausstattung.

Raumverzeichnis

Als Top Level Dokument benötigen wir somit ein Verzeichnis aller Räume mit IT-Ausstattung oder manueller Verarbeitung von Daten, und zwar mit Angaben zur Lage – z. B. mittels Raumnummer und Verweis auf einen Bauplan.

Raumbeschreibung

Je genutzter Räumlichkeit sollten wir folgende Informationen bereitstellen (s. Abbildung 5):

– Beschreibung der baulichen Gegebenheiten: Beschaffenheit von Wänden, Decken, Türen und Fenster,

– Beschreibung der vorhandenen Schnittstellen wie z. B. Strom-Zuführung, Netzwerk-Anschlüsse, ggf. Wasseranschlüsse – jeweils mit Angabe der Grenzlasten,

– Beschreibung der vorhandenen Ausstattungselemente wie z. B. die schon genannten Warn-, Melde- und Löschsysteme, die Zutrittskontrolle,

– Benennung der Rollen, die für die Infrastruktur zuständig sind – z. B. für die Störungsannahme, Alarmzentrale, Feuerwehr – und entsprechende Kontaktangaben

– div. Aufzeichnungen über die Inbetriebnahme, Fehlerzustände und Störungen, Wartungsvorgänge.

Die ersten drei Elemente sind meist detaillierten Baubeschreibungen bzw. Raumplänen zu entnehmen. Für jede Schnittstelle und jedes Ausstattungselement benötigen wir einen Verweis auf weiterführende Dokumente, in der diese Elemente beschrieben sind. Bei den baulichen Gegebenheiten, den Schnittstellen und sonstigen Ausstattungen benötigen wir vor allem auch eine Angabe über die Grenzlasten, z. B. max. zulässige Gewichte, Netzbelastbarkeit, usw.

Das Raumverzeichnis und die Raumbeschreibungen zu erstellen und zu pflegen, ist Aufgabe der zuständigen Rollen „Manager-1“ bzw. „Manager-2“.

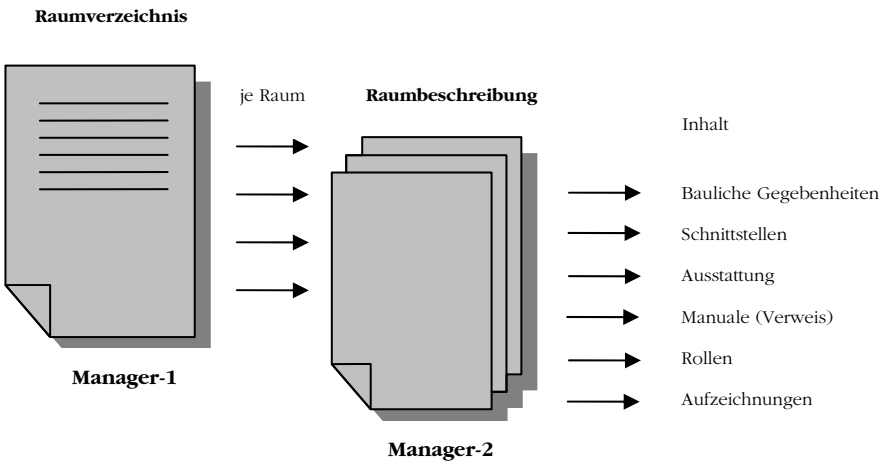

Abbildung 5: Dokumentation zur Infrastruktur

Einsatzumgebung

Die im Zusammenhang mit einem IT-System definierte Organisation (Rollen und ihre Arbeitsanweisungen), das beauftragte Personal und die genutzte physische Infrastruktur bezeichnet man häufig als *Einsatzumgebung* des IT-Systems.

Diese ist nicht zu verwechseln mit der *IT-Umgebung* z. B. eines Software-Produktes, die die zur Nutzung des Produktes erforderliche Plattform (Hardware, Betriebssystem und sonstige Komponenten) meint. Sie ist besonders wichtig, wenn es darum geht,

- ein IT-System nach Sicherheitskriterien zu evaluieren und zu zertifizieren[6],
- ein zertifiziertes IT-System zu nutzen und dazu die der Zertifizierung zugrunde liegende IT-Umgebung in der Praxis zu realisieren.

3.6 Software-Anwendungen

IT-Systeme sind kein Selbstzweck, sondern unterstützen ihren Betreiber bei der Erbringung von Dienstleistungen für sich selbst oder seine Kunden: z. B. Gehaltsabrechnung, Software-Produktion und -Verteilung, Bereitstellung von Datenbanken, Abwicklung von Online-Transaktionen, eShop-Anwendungen.

6 z. B. nach den ITSEC oder den Common Criteria

Software-Anwendungen

Hierzu bedient sich der Betreiber bestimmter Software-Anwendungen, die – meist verteilt – auf seinen IT-Systemen laufen. Solche Software-Anwendungen verlassen sich oft auf Sicherheitseigenschaften der IT-Systeme und Netzwerke, auf denen sie laufen, realisieren vielfach aber auch eigene, anwendungsbezogene Sicherheitsfunktionen[7].

Um solche Überlegungen in unsere konzeptionellen Arbeiten einbeziehen zu können, benötigen wir eine Liste der zu berücksichtigenden Software-Anwendungen mit dem Namen und dem Zweck der SW-Anwendung sowie dem Namen des Managers dieser Anwendung, sodann zu jeder SW-Anwendung eine spezifische Dokumentation mit zumindest folgendem Inhalt (s. Abbildung 6):

- Beschreibung der Anwendung,
- zuständige weitere Rollen für diese Anwendung – z. B. für die Installation, die Administration, den Betrieb, die Fehlerbehandlung und die Wartung,
- Art und Umfang der Schnittstellen zu anderen Anwendungen,
- Liste der IT-Systeme, auf denen die Anwendung läuft, sowie eine Angabe zur erforderlichen Netzwerkinfrastruktur,
- Voraussetzungen, die auf diesen IT-Systemen bzw. im Netzwerk erfüllt sein müssen, damit die SW-Anwendung lauffähig ist,
- Verweis auf die Dokumentation (Manuale) für die Nutzung der SW-Anwendung und für die Installation, Administration, Fehlerbehandlung, Wartung,
- div. Aufzeichnungen über die Inbetriebnahme, Fehlerzustände, Wartungsschritte, usw.

---

7 Typische Beispiele sind Datenbank-Managementsysteme (DBMS), die zusätzlich zur Zugriffskontrolle des Betriebssystems einen eigenen Zugriffsschutz bis auf einzelne Felder von Datenbanken realisieren können.

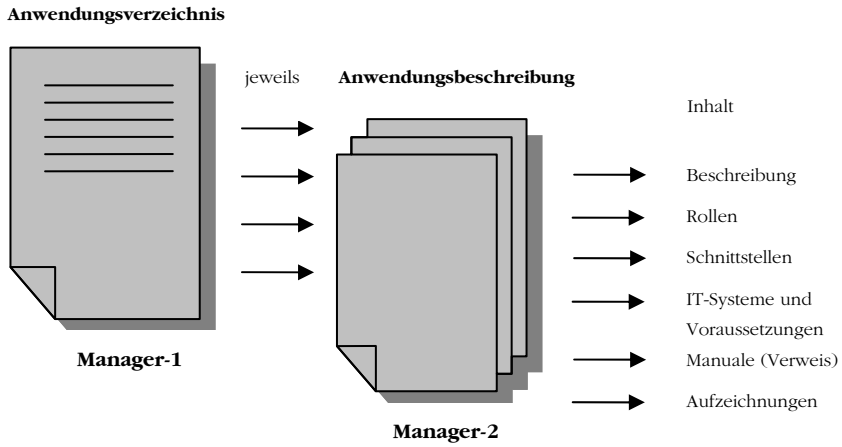

Abbildung 6: Dokumentation zu SW-Anwendungen

3.7 IT-Verbund

Als *IT-Verbund* eines Unternehmens bezeichnen wir die Zusammenfassung aller

- IT-Systemen einschließlich der Netzwerkkomponenten und Netzwerkübergänge,
- auf den IT-Systemen laufenden Software-Anwendungen.

Einsatzumgebung Die Einsatzumgebung des IT-Verbunds enthält die Einsatzumgebungen der einzelnen IT-Systeme – kann jedoch umfassender sein: Es wird stets Rollen und Infrastruktur-Elemente geben, die den IT-Verbund als Ganzes betreffen und bei der Behandlung der Einzelsysteme nicht betrachtet wurden.

Dokumentation Die Dokumentation des IT-Verbunds umfasst folglich die Dokumentation aller dazu gehörenden IT-Systeme, den Vernetzungsplan sowie alle Organisations- und Infrastruktur-Elemente, die den IT-Verbund als Ganzes betreffen.

IV-System Als **i**nformations**v**erarbeitendes System, kurz: *IV-System,* bezeichnet man gelegentlich einen IT-Verbund mit seiner Einsatzumgebung und seiner Dokumentation.

3.8 Geschäftsprozesse

Ein IT-Verbund stellt ein Hilfsmittel zur Unterstützung der Geschäftsprozesse eines Unternehmens dar:

Geschäftsprozess

Ein *Geschäftsprozess* ist eine Abfolge von miteinander vernetzten Tätigkeiten, die von Personen in einem Unternehmen – ggf. unter Nutzung des IT-Verbunds und ggf. auch unter Beteiligung von Externen – ausgeführt werden und das Ziel haben, eine beabsichtigte Leistung bzw. ein gewünschtes Ergebnis zu erbringen.

Manager

Für jeden Geschäftsprozess als Ganzes ist die Rolle eines Verantwortlichen festzulegen, der für die Dokumentation, den Betrieb des Geschäftsprozesses und die Erbringung der Leistung sowie für Änderungen zuständig ist – diese Aufgaben natürlich an weitere Personen delegieren kann.

Es macht hier ebenfalls Sinn, eine Liste der Geschäftsprozesse anzulegen, in der die Namen der Prozesse, ihr jeweiliger Zweck (grob) und die Rolle eines zuständigen Managers festgehalten sind.

Ein Geschäftsprozess wird in Teilen – möglicherweise sogar vollständig – elektronisch abgewickelt. Sehr oft wird es aber auch Anteile von Geschäftsprozessen geben, die manuell von dazu beauftragten Personen bearbeitet werden. Insbesondere die Aufgaben der Einrichtung und Konfiguration eines Geschäftsprozesses, das Änderungsmanagement, die Einstellung eines Geschäftsprozesses sind überwiegend manuelle Tätigkeiten.

Nun zur Dokumentation von Geschäftsprozessen (s. Abbildung 7):

Verträge

Den Geschäftsprozessen quasi übergeordnet sind Verträge, Vereinbarungen, Aufträge oder Vorgaben zum Gegenstand der Leistungserbringung und ihrer Kennzahlen. Sie beinhalten die operationellen Zielvorgaben eines Geschäftsprozesses.

Verfahrensbeschreibung

Man erkennt, dass das für die Sicherheitsanalyse wichtigste Dokument zu einem Geschäftsprozess seine Verfahrensbeschreibung sein dürfte: Hierin sind

- die Zielvorgaben und erwarteten Ergebnisse (Kennzahlen),
- die beteiligten Rollen,
- die vorgesehen Abläufe,
- die genutzten Einrichtungen (etwa der IT-Verbund) sowie
- Schnittstellen zu anderen Geschäftsprozessen beschrieben.

Dokumentation

Zu einem Geschäftsprozess gehören weiterhin Aufzeichnungen über

- die *tatsächlichen* Ergebnisse bzw. die *tatsächliche* Leistungserbringung des Geschäftsprozesses,
- die Nutzung des Geschäftsprozesses,
- Beanstandungen und Fehlerzustände und deren Behebung.

Diese Informationen dienen Nachweis- bzw. Beweiszwecken, aber auch der stetigen Verbesserung und zielgerichteten Anpassung eines Geschäftsprozesses.

Man beachte noch den Unterschied: Bei einer *Verfahrensbeschreibung* geht es um die Beschreibung eines Verfahrens bzw. Prozesses als Ganzes; eine *Arbeitsanweisung* dagegen bezieht sich auf die Tätigkeiten einer speziellen Rolle *innerhalb* eines Geschäftsprozesses oder für mehrere Geschäftsprozesse.

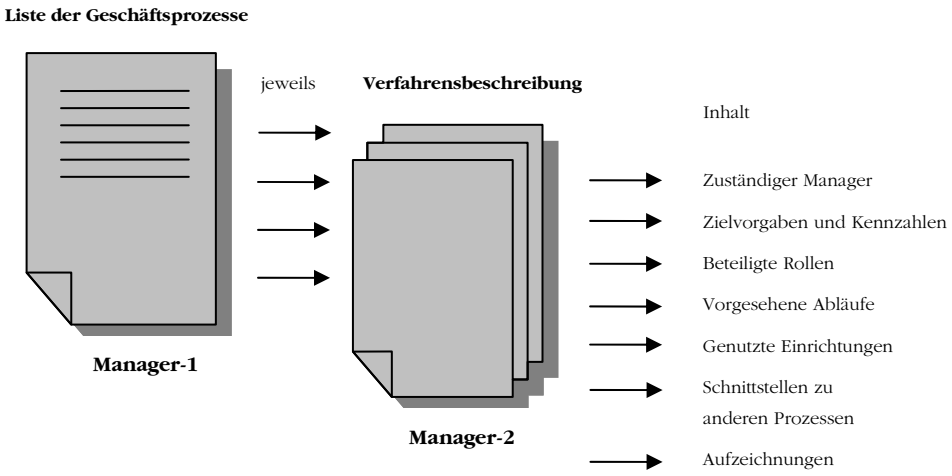

Abbildung 7: Dokumentation zu den Geschäftsprozessen

Anmerkung: Zwei andernorts verwendete Begriffe wollen wir kurz einordnen, aber wegen der Gefahr von Missverständnissen nicht weiter verwenden:

Gelegentlich findet man die Bezeichnung *IT-Verfahren*, die im Grunde für einen Geschäftsprozess steht, der durch IT unterstützt wird. Unser Begriff eines Geschäftsprozesses geht jedoch insofern weiter, als eine IT-Unterstützung nicht zwingend ist.

Der Teil eines Geschäftsprozesses, der mittels der IT abgewickelt wird, wird gelegentlich als *IT-Anwendung* bezeichnet – diese ist aber nicht notwendigerweise mit einer *Software-Anwendung* gleichzusetzen; vielmehr kann sich die IT-Anwendung mehrerer Software-Anwendungen und auch externer Daten bedienen.

4 Sicherheitsziele auf allen Ebenen

Ziele, die sich auf die Sicherheit von Informationen und Daten, IT-Systemen sowie Geschäftsprozessen beziehen, nennen wir einfach *Sicherheitsziele*. Welche Ziele das sein können und wie sie sich im Einzelnen darstellen, behandeln wir jetzt.

4.1 Informationen und Daten

Auf der Ebene von *Informationen* und *Daten* werden üblicherweise drei grundlegende Sicherheitsziele genannt: Vertraulichkeit, Verfügbarkeit, Integrität – etwas präziser:

- die Vertraulichkeit von Informationen,
- die Integrität von Daten,
- die Verfügbarkeit von Daten(trägern).

Wer glaubt, dass man mit dieser Aufzählung schon alles erledigt hat, irrt! Diese Aufzählung ist zu oberflächlich, um darauf etwa ein Sicherheitskonzept aufbauen zu können. Insbesondere fehlt ein wichtiges Ziel! Schauen wir uns die Begriffe deshalb etwas genauer an:

Vertraulichkeit

Die Eigenschaft einer Information, nur dem beabsichtigten Personenkreis – den „Befugten“ – bekannt zu sein, bezeichnen wir als *Vertraulichkeit*[8].

Wie man unschwer erkennt, setzt dies voraus, dass jemand den Kreis der Befugten festlegt. Hierfür gibt es im Wesentlichen die folgenden Alternativen:

---

8 Es ist klar, dass die Vertraulichkeit eine Eigenschaft oder ein Attribut einer *Information* ist; liegt eine Information in Datenform vor, so kann sich die Forderung nach Vertraulichkeit natürlich sinngemäß auch auf die Daten (und Datenträger) übertragen – dies ist aber nicht zwingend, wie man am Beispiel verschlüsselter Informationen leicht erkennen kann: Die sich als Ergebnis der Verschlüsselung ergebenden Daten müssen nicht mehr „vertraulich“ bleiben.

– der „Urheber“ oder „Eigentümer“ der Information – derjenige, bei dem die Information entsteht, der sie als Erster „besitzt“ – oder
– eine zentrale Stelle, der die Informationen zur Festlegung der Befugten *vor* einer möglichen Verarbeitung bzw. Weitergabe vorgelegt werden[9].

DAC, MAC

Im ersten Fall spricht man von einer *benutzerbestimmbaren Zugriffskontrolle*[10], im zweiten Fall von einer *vorgeschriebenen Zugriffskontrolle*[11].

Berechtigungskonzept

In der Praxis gibt es eine Reihe von Mischformen dieser beiden grundsätzlichen Formen der Zugriffskontrolle. Wir wollen dieses Thema hier nicht näher behandeln, halten jedoch fest, dass wir bei der Konzeption der Sicherheit diesbezügliche Vorüberlegungen anstellen müssen. Man spricht hier von einem *Berechtigungskonzept*. Mehr zum Management von Berechtigungen erfahren Sie im Abschnitt „11.3 Zugriffskontrolle“.

Verlust der Vertraulichkeit

Vom *Verlust der Vertraulichkeit* sprechen wir, wenn vertrauliche Informationen Unbefugten zur Kenntnis gelangen. Drei Beispiele:

– In einem Netzwerk werden Datenpakete auf dem Übertragungswege von Unbefugten abgehört.
– Bei einem ansonsten vor Verlust der Vertraulichkeit geschützten IT-System werden tägliche Backups der Daten gezogen, die Backup-Medien jedoch nicht sicher aufbewahrt, d. h. Unbefugte können diese leicht entwenden bzw. sich Kopien erstellen.
– Durch Sicherheitslücken in einem IT-System können Hacker dieses IT-System penetrieren und vertrauliche Daten in großer Menge stehlen.

---

9 Ein solche Festlegung findet oft in Form einer „Einstufung“ statt: Informationen werden als „offen“ oder „Firmen-vertraulich“ oder „Nur für Mitarbeiter des Projektes xyz“ klassifiziert; im staatlichen Geheimschutzbereich findet man Klassen wie „vertraulich“, „geheim“ oder „streng geheim“.

10 Im Englischen: *Discretionary Access Control*, abgekürzt: DAC.

11 Im Englischen: *Mandatory Access Control*, abgekürzt: MAC.

Ein Grundproblem der Vertraulichkeit ist, dass man den Daten einen Verlust der Vertraulichkeit nicht ansehen kann. Es kann also leicht passieren, dass die Vertraulichkeit längst nicht mehr gegeben ist, die Befugten dies jedoch nicht wissen.

Was kommt als Ursache für den Verlust der Vertraulichkeit in Frage? Hier ist zu unterscheiden zwischen

- der Weitergabe von vertraulichen Informationen durch *Befugte* an Unbefugte,
- Schwachstellen in Systemen oder Verfahren, aufgrund derer Unbefugte an vertrauliche Informationen gelangen.

Bei der Weitergabe an Unbefugte muss man unterscheiden, ob dies

- unbeabsichtigt – wenn auch vielleicht fahrlässig – oder
- beabsichtigt geschieht.

Zu den Themen *Schwachstellen* und *Fahrlässigkeit* finden Sie Informationen in Abschnitt „5.5 Ergänzendes zur Schwachstellenanalyse“. *Beabsichtigte Handlungen* wollen wir stets unter *Missbrauch* einordnen, d. h. hier handelt es sich um die „missbräuchliche Weitergabe“ von Informationen – ein eigener „Tatbestand“, mit dem wir uns noch beschäftigen werden.

Integrität

Die *Integrität* ist die Eigenschaft von Daten (!), nur in zulässiger Weise durch Befugte geändert worden zu sein.

Unter *Ändern* verstehen wir das Abändern vorhandener Daten, das teilweise oder vollständige Löschen[12] von Daten, das Hinzufügen neuer Daten.

Die obige Definition von Integrität setzt voraus, dass die betrachteten Daten zu einem bestimmten Zeitpunkt als *integer* festgestellt, die zulässigen Änderungen als solche definiert wurden und der Kreis der Befugten festgelegt wurde. Für diese Festlegungen gibt es ähnliche Alternativen wie bei der Vertraulichkeit: Man überlässt sie dem Eigentümer der Daten oder einer zentra-

12 Gemeint ist hier immer das Löschen von Daten in einer Datenstruktur (etwa einer Datei), ohne die Datenstruktur selbst zu löschen. Integrität ist also genau genommen eine Eigenschaft des *Inhalts* einer Datenstruktur.

len Instanz. Auch diese Überlegungen finden ihren Niederschlag im Berechtigungskonzept.

In einem IT-System können *Unbefugte* z. B. mit Mitteln der Zugriffskontrolle davon abgehalten werden, Daten zu ändern. Schwierig wird es, *Befugte* so zu überwachen, dass sie nur *zulässige* Änderungen vornehmen. Hier greifen Mechanismen unter den Überschriften Vier-Augen-Prinzip, schriftliche Nachweise und Plausibilitätskontrollen.

Verlust der Integrität

Ein Verlust der Integrität liegt dann vor, wenn die Daten entweder a) durch Befugte in unzulässiger Weise oder b) durch andere Ursachen (unzulässig) geändert worden sind.

a) Bei der unzulässigen Änderung von Daten durch *Befugte* muss man wieder danach unterscheiden, ob dies unbeabsichtigt (durch Bedienungsfehler, auch vielleicht fahrlässig) oder beabsichtigt geschieht. Letzteres wollen wir als „missbräuchliche Änderung“ von Daten bezeichnen.

b) Zu den anderen Ursachen zählen wir mehr zufällige Ursachen wie Fehlfunktionen der IT-Systeme oder Störungen bei der Datenübertragung sowie die Manipulation durch Unbefugte.

Typisch für Computer-Viren und Computer-Würmer ist die Verletzung der Integrität von *Software*. Somit helfen Maßnahmen unter der Überschrift „Virenschutz“, die Integrität von Software zu wahren. Weitere wichtige Maßnahmen sind solche, die die Verletzung der Integrität von Daten erkennen lassen: Signatur- und Verschlüsselungsverfahren. Fehlerkorrigierende Codes sind Verfahren, um z. B. störungsbedingte Änderungen an Daten auf dem Übertragungsweg oder am Speicherort erkennen und in beschränktem Maße automatisch beheben zu können.

Widmen wir uns noch der Frage, wann eine Verletzung der Integrität von Daten bemerkt wird: offensichtlich *frühestens* dann, wenn man sie erneut verwenden will; eine besonders „raffinierte“ Daten-Manipulation kann möglicherweise erst zu einem sehr späten Zeitpunkt erkannt werden – etwa anhand von untypischem Verhalten von Software oder bei unsinnigen Ergebnissen.

Verfügbarkeit

Unter *Verfügbarkeit* wird die Eigenschaft von Daten verstanden, für Befugte bei Bedarf und dann in akzeptabler Zeit zur Verfügung zu stehen.

Ein „Bedarf“ liegt immer dann vor, wenn ein Zugriff als Teil der zulässigen Verarbeitung erfolgen soll. „In akzeptabler Zeit“ meint, dass die gewünschten Daten mit einer noch als zulässig akzeptierten Verzögerung bereitstehen.

Auch hier ist es möglich, dass die gerade noch akzeptierte Verzögerung durch den Eigentümer der Daten oder von einer zentralen Instanz festgelegt wird. In der Praxis liegt meistens der zweite Fall vor.

Da Daten stets auf Datenträgern vorliegen, ist die Verfügbarkeit von Daten immer an die Verfügbarkeit von Datenträgern gebunden. Andererseits ist dies nicht hinreichend: Ein Datenträger (z. B. eine Festplatte) kann im gewünschten Umfang verfügbar sein, aber die gewünschten Daten sind – z. B. durch Löschung – nicht mehr verfügbar.

Typische Maßnahmen, um einen bestimmten Grad an Verfügbarkeit zu erreichen und aufrechtzuerhalten, stellen Redundanzmaßnahmen (mehrfache Vorhaltung von Daten auf dem gleichen oder verschiedenen Datenträgern) und bestimmte Verfahren von Betriebssystemen (Verwaltung konkurrierender Zugriffe, um Deadlocks beim Zugriff zu vermeiden) dar. Mehrfache Vorhaltung von Daten erreicht man im einfachsten Fall durch Erzeugen von Kopien auf dem gleichen Datenträger, dann aber durch parallele Speicherung auf mehreren Plattenspeichern, regelmäßiges Backup der Daten auf separaten Datenträgern sowie Nutzung von Systemen für die Langzeitarchivierung.

Man beachte hierbei auch wieder den Verfügbarkeitsaspekt der Daten*träger*.

Verlust der Verfügbarkeit

Die Ursachen für einen *Verlust der Verfügbarkeit* von Daten können vielfältig sein. Zunächst kann der Verlust dadurch begründet sein, dass die gewünschten Daten für den Nutzer nicht mehr vorhanden sind, d. h. entweder gelöscht bzw. vernichtet wurden oder kein ausreichendes Zugriffsrecht mehr vorhanden ist. Haben zu dieser Situation absichtliche Handlungen von Befugten geführt, sprechen wir von *missbräuchlicher Vorenthaltung* von Daten – ein eigener Missbrauchs-Tatbestand. Somit verbleiben als Ursachen für diese Form des Verlustes der Verfügbarkeit von Daten noch

- unbeabsichtigte Handlungen von Personen (Befugte oder Unbefugte) wie z. B. Bedienungsfehler, Fehler bei den Wartungsmaßnahmen, Stichwort: Fahrlässigkeit,
- technische Defekte,

– Manipulationen durch Unbefugte.

Eine andere Form des Verlustes der Verfügbarkeit von Daten liegt vor, wenn die Daten zwar vorhanden, aber nicht in akzeptabler Zeit zur Bearbeitung bereitgestellt werden können. Dies kann an nicht ausreichender Verfügbarkeit des IT-Systems oder anderer Prozesse – z. B. der zu zeitaufwändigen Daten-Wiederherstellung vom Backup-Medium – liegen: Mit diesen Fällen der *Verfügbarkeit von Systemen* beschäftigen wir uns später.

Bitte beachten Sie, dass es bei der Verfügbarkeit *nicht* darauf ankommt, ob die bereitgestellten Daten unverändert sind – dies wäre ein Integritätsaspekt, im Extremfall: Wird unzulässigerweise der *Inhalt* einer Datei gelöscht (z. B. durch Überschreiben mit Blanks), bleibt aber die Datenstruktur „Datei" als solche vorhanden, dann wurde die Integrität der Daten verletzt. Wird die Datenstruktur „Datei" gelöscht[13], ist die Verfügbarkeit der Daten verletzt. Diese Gegenüberstellung macht deutlich, dass wir vielfach die Verfügbarkeit von Datenstrukturen meinen.

Der Verlust der Verfügbarkeit wird meist recht schnell entdeckt – *spätestens* dann, wenn die Daten wieder bearbeitet werden sollen.

Authentizität von Daten

Gelegentlich wird ein Sicherheitsziel „Authentizität von Daten" definiert und so verstanden, dass

– ihre Herkunft (Absender, Erzeuger) sicher nachgewiesen werden kann und

– die Übereinstimmung der Daten mit ihrem „Original" (beim Absender, Erzeuger) gewahrt bleibt.

Man erkennt leicht, dass der zweite Anstrich unser bekanntes Sicherheitsziel der Integrität beschreibt ist. Der erste Anstrich dagegen ist ein bisher nicht formuliertes Sicherheitsziel. Wir werden es im Zusammenhang mit Sicherheitszielen für Geschäftsprozesse (s. Abschnitt 3.8) behandeln.

---

13 Damit ist ja nicht zwingend die Löschung der Daten verbunden: Man denke an die „Löschung" von Dateien in Windows-Systemen, bei der die eigentlichen Daten auf dem Speicher auch noch nach dem „Löschen der Datei" vorhanden sind, teilweise sogar als Datei wiederhergestellt werden können.

Unsere Bemerkungen zum Zeitpunkt der Entdeckung der verschiedenen Verluste können wir in der Abbildung 8 zusammenfassen:

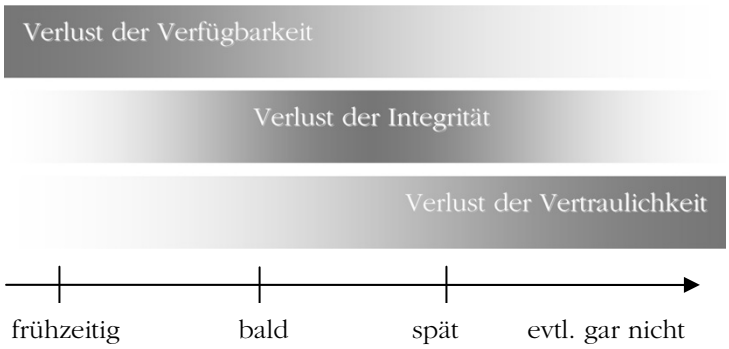

Abbildung 8: Zeitpunkt der Entdeckung eines Verlustes

Missbrauch

Schlussendlich tragen wir noch als wichtiges Sicherheitsziel die Vermeidung von Missbrauch nach: Ein Missbrauch von Informationen bzw. Daten liegt vor, wenn diese durch *Befugte*

- an Unbefugte weitergegeben,
- in unzulässiger Weise geändert oder
- anderen Befugten unzulässig vorenthalten werden.

Innentäter

Vor dem Hintergrund der bekannten Innentäter-Problematik, die heutzutage immer noch den größten Anteil an der Schadenstatistik[14] trägt, ist es unabdingbar, die Vermeidung von Missbrauch in die Risikoanalyse und Risikobewertung aufzunehmen, jedenfalls sie nicht in der üblichen Aufzählung von „Verlust der Vertraulichkeit, Integrität und Verfügbarkeit“ zu verstecken.

Einen Missbrauch von Daten durch technische Maßnahmen *in einem IT-System* abfangen oder auch nur entdecken zu wollen, ist schwierig, teilweise gar unmöglich, da es sich ja immer um Aktionen von Befugten handelt. Außerhalb der IT-Systeme gilt dies umso mehr: Es gibt keine absolut wirksame Sicherheitsmaßnahme, um z. B. eine mündliche Weitergabe von geheimen Informationen an Unbefugte auszuschließen. Man kann zwar ar-

[14] Genauer gesagt: am Schadenvolumen. Man geht von einem Anteil von 60-85 % aus.

beitsvertragliche Regelungen mit Strafandrohungen vorsehen – die Wirksamkeit ist jedoch sehr begrenzt.

Gerade weil dies sehr pessimistisch klingt, ist es wichtig, die Risiken des Missbrauchs von Daten genau zu beleuchten; diese Risiken zu ignorieren heißt, sich nur auf Nebenkriegsschauplätzen zu tummeln – wozu dann der Aufwand?

Skalierung

Für die nunmehr vier Sicherheitsziele – Vertraulichkeit, Integrität, Verfügbarkeit, Missbrauchsschutz – bei Informationen bzw. Daten reicht es oft nicht aus, sie im Sinne von „Ja“ oder „Nein“ zu fordern. Vielmehr kann es Abstufungen bzw. Skalierungen geben:

Dies ist besonders leicht bei der *Verfügbarkeit* einsehbar, die in % der betrachteten Zeit angegeben wird. Daten sollen z. B. in 99,75 % der Zeit verfügbar sein, was einen Ausfall von ca. 20 h pro Jahr erlaubt.

Bei der *Vertraulichkeit* von Informationen ist es nicht ganz so einfach: Unsere Sprache legt uns nahe, dass etwas entweder vertraulich oder nicht vertraulich ist. Stufungen sind nicht erkennbar. Denkt man jedoch an die Informationen eines Unternehmens, so stellt man fest: Es gibt Informationen, bei denen der Verlust der Vertraulichkeit einen höheren Schaden verursacht als bei anderen Informationen. Aus dieser Überlegung zu den *Folgen des Verlustes* könnte jedes Unternehmen für sich Stufen der Vertraulichkeit ableiten: Man gibt sich beispielsweise drei Stufen für den verursachten Schaden vor (kein Schaden, tolerierbarer Schaden, nicht mehr tolerierbarer Schaden) und ordnet diesen Klassen Stufen der Vertraulichkeit zu – etwa: offen, firmen-vertraulich, „top secret“. Diese Stufen sind aufsteigend angeordnet. Man kann jedoch auch ganz anders vorgehen und Informationen nach Sachgebieten oder den Befugten klassifizieren: Vorstandsinformationen, Kundendaten, Entwicklungsgeheimnisse. Diese Klassen kann man nicht unbedingt aufsteigend anordnen, sie stehen eventuell sogar beziehungslos nebeneinander. Für jede Klasse können aber eigene Vorschriften zur Geheimhaltung existieren.

Bei Behörden bzw. bei staatlichen Verschlusssachen nutzt man eine Kombination dieser beiden Methoden: Es werden

– hierarchische Stufen wie „offen“, „vertraulich“, „geheim“, „streng geheim“ festgelegt, die sich an dem durch einen Bruch der Vertraulichkeit verursachten Schaden orientieren,

– Informationen bei Bedarf zusätzlich klassifiziert nach den Befugten oder nach Sachgebieten.

Solche Einstufungen und Klassifizierungen machen nur Sinn, wenn es praktikable Vorschriften bzw. Sicherheitsrichtlinien gibt, wie mit den entsprechenden Informationen umzugehen ist. Aus solchen Vorschriften müssen sich Maßnahmen ableiten lassen. Als Beispiel sei die Stufe „vertraulich" bei staatlichen Verschlusssachen genannt, ab der eine Verschlüsselung von Daten bei der Übertragung zwingend ist; die Verschlüsselung darf nur mit einem von einer zentralen Stelle zugelassenen Verfahren erfolgen.

Bei der *Integrität* von Daten wird es mit Stufen noch schwieriger: Auch hier kann man keine direkte Stufung angeben, auch eine Betrachtung von Schäden bei Verlust der Integrität ist eher unhandlich. Bei der Integrität von Daten hat man auf der Maßnahmenseite oft nur die *Entdeckung* von Integritätsverlusten zur Verfügung. Dabei geht es um störungsbedingte, unbefugte und unzulässige Änderungen. Hieran könnte man 3 Integritätsstufen orientieren:

– „normal": „Entdeckung störungsbedingter (Bit-)Fehler",
– „mittel": „Entdeckung jeder Art von unbefugter Änderung",
– „hoch": „Entdeckung jeder Art von unzulässiger Änderung".

Für „normal" würde dann unsere übliche Datenspeicherung auf Speichermedien ausreichen, für „mittel" könnten etwa Methoden der elektronischen Signatur eingesetzt werden, bei „hoch" würde man zusätzlich eine Zugriffskontrolle und das Vier-Augen-Prinzip bei der Bearbeitung der Daten verlangen. Es sei hier angemerkt, dass man Integritätsklassen auch auf andere Weisen definieren kann, z. B. durch „Einstufungen" ähnlich wie beim staatlichen Geheimschutz.

Bei der Vermeidung von *Missbrauch*, die sich ja auf Vertraulichkeit, Verfügbarkeit und Integrität bezieht, koppelt man die zuvor festgelegten Einzelmaßstäbe.

Fazit: Im Grunde kann man für jede Information bzw. jedes Datum ein eigenes Profil mit abgestuften Sicherheitszielen aufstellen.

Gruppierung zu Objekten

Beim Sicherheitskonzept würde dies aber einen enormen Aufwand nach sich ziehen. Man denke nur an die „Menge" von Unternehmensdaten und -dateien. Besser ist es, Informationen bzw. Daten mit gleichem oder vergleichbarem Profil zu gruppieren: Dazu eignet sich meist die Zusammenfassung nach Organi-

sationseinheiten – also etwa die Daten der Entwicklungsabteilung, die Daten der Personalabteilung, usw.), nach Kunden oder Projekten – oder auch nach der Zugehörigkeit zu Geschäftsprozessen. Dennoch wird es immer einzelne Informationen und Daten geben, die individuell zu behandeln sind. Mit *Informations-* bzw. *Datenobjekten* meinen wir entweder solche individuell zu behandelnde Informationen bzw. Daten oder eben entsprechende Gruppen von Informationen bzw. Daten.

Datensicherheit

Wir sprechen von *Informations-* bzw. *Datensicherheit* in einem Unternehmen, wenn für jedes betrachtete Informations- bzw. Datenobjekt die Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Verhinderung von Missbrauch in der gewünschten Zusammenstellung und Abstufung erreicht und aufrechterhalten werden.

Man erkennt hier, dass diese Definition keine absolute Sicherheit fordert und die Sicherheit immer eine individuelle, d. h. auf eine Institution angepasste ist.

Datenschutz

Anmerkung: Man beachte an dieser Stelle, dass Datensicherheit in diesem Sinne zunächst nichts mit *Datenschutz* zu tun hat: Hierunter verstehen wir den Schutz von *personenbezogenen* Daten als Teil der Privatsphäre entsprechend den Anforderungen der Datenschutzgesetze. Diese Anforderungen kann man grob zusammenfassen als

- Gebot der Datensparsamkeit und Datenvermeidung: Daten sollen nur in dem Umfang erhoben werden, wie es für den vorgesehenen Zweck notwendig ist, sowie
- Forderung nach Zweckbindung von Daten: Erhobene Daten dürfen ausschließlich für den beabsichtigten Zweck verwendet werden.

Als „Zweck“ sind dabei zulässig

- entweder gesetzlich definierte Zwecke (z. B. durch die Steuer- und Sozialgesetzgebung) oder
- solche, bei denen die Betroffenen der Verwendung ihrer personenbezogenen Daten zugestimmt haben.

Solche Anforderungen lassen sich nicht immer und nicht allein als Forderungen an die Datensicherheit im obigen Sinne interpretieren.

4.2 IT-Systeme und IV-Systeme

Diskutieren wir nun Sicherheitsziele für *IT-Systeme*. Eine Vertraulichkeit als Ziel gibt es nicht, da dies ein informationsbezogenes Ziel ist. Anders sieht es mit Integrität, Verfügbarkeit und Vermeidung von Missbrauch aus.

System-Verfügbarkeit

Mit *Verfügbarkeit eines IT-Systems* bezeichnen wir die Eigenschaft, die beabsichtigte bzw. zugesicherte Funktion für jeden befugten Nutzer bei Bedarf und in akzeptabler Zeit zur Verfügung stellen zu können. Welche Zeit akzeptabel ist, kann sich von Funktion zu Funktion, von Nutzer zu Nutzer unterscheiden, wird aber meist zentral festgelegt.

Der Verlust der Verfügbarkeit eines IT-Systems kann folgende Ursachen haben:

- zu geringe Leistungsfähigkeit (Performance),
- Elementarereignisse mit der Folge von Systemausfall,
- technisches Versagen aufgrund minderer Qualität, ungeeigneter Umgebungsbedingungen oder Alterung – mit der Folge von Systemausfall oder reduzierter Performance,
- bewusste oder zumindest fahrlässige Handlungen von Personen wie Manipulation, Sabotage bzw. Zerstörung des Systems, DoS-Attacken[15].

Beispiel: Die Verfügbarkeit eines Routers kann durch technische Defekte oder Störungen, durch betriebsbedingtes hohes Datenaufkommen, aber auch durch DoS-Attacken gemindert sein.

Die Klasse möglicher Gegenmaßnahmen ist sehr groß und reicht von zuverlässigen und ausfallsicheren IT-Systemen, Maßnahmen zur Fehlererkennung und Fehlerüberbrückung, bis hin zur Zugriffskontrolle zur Abwehr illegaler Aktionen und zur Begrenzung von Betriebsmitteln – z. B. das Load Balancing.

System-Integrität

Die *Integrität eines IT-Systems* ist dann gegeben, wenn dessen beabsichtigte bzw. zugesicherte Funktionen nicht unzulässig geändert wurden.

---

15 Denial of Service: Attacken gegen Netzwerke, durch die die Netzwerkdienste so überlastet werden, dass sie von den normalen Nutzern nur noch beschränkt oder gar nicht mehr abgerufen werden können.

Wie bei der Daten-Integrität setzt dies voraus, dass zu einem bestimmten Zeitpunkt das IT-System als *integer* festgestellt wurde und jede Änderung grundsätzlich entweder als zulässig oder unzulässig klassifiziert werden kann.

Die System-Integrität bezieht sich auf die Hardware und Firmware wie auch auf die laufenden, von der Software gesteuerten Prozesse[16].

Der Verlust der Integrität eines IT-Systems kann z. B. durch folgende Ursachen bedingt sein:

- Elementarereignisse mit der Folge von Systemausfall,
- technisches Versagen aufgrund minderer Qualität, ungeeigneter Umgebungsbedingungen oder Alterung,
- bewusste oder zumindest fahrlässige Handlungen von Personen,

jeweils mit der Folge, dass sich das IT-System anders als beabsichtigt oder zugesichert verhält.

Unbefugte können die System-Integrität verletzen, indem sie sich z. B. physischen Zugang zu dem System verschaffen und entsprechende Änderungen, z. B. Austausch von Hardware, vornehmen. Im Zuge der Anbindung an das Internet oder über Fernwartungssysteme können Unbefugte solche Integritätsverletzungen auch „aus der Ferne“ begehen: in laufende Prozesse eingreifen, bis auf die Ebene von Firmware Änderungen vornehmen – wenn auch nicht direkt Hardware austauschen.

Zugriffskontrolle und Zutrittskontrolle sind hier wichtige Sicherheitsmaßnahmen zur *Verhinderung* des Integritätsverlustes; Maßnahmen zur *Entdeckung* von Integritätsverletzungen sind Funktionskontrollen, Systeminspektionen, Software-Abgleich.

System-Missbrauch

Die missbräuchliche Verwendung und die unbefugte Nutzung eines IT-Systems sind Tatbestände, die wir als *System-Missbrauch* bezeichnen. Die Vermeidung eines solchen Missbrauchs kann ein Sicherheitsziel für ein IT-System sein.

---

16 Hier wird es jetzt schwierig: Die Änderung gespeicherter Software (Software sind Daten!) haben wir schon bei der Datenintegrität behandelt. Wird aber ein Programm gestartet und initiiert man damit einen *Prozess*, geht es nicht mehr um die Datendarstellung des Programms, sondern um sein Verhalten.

Gruppierung zu Objekten

Ähnlich wie für die Daten gilt auch für die IT-Systeme eines Unternehmens, dass für sie unterschiedliche Sicherheitsziele – und diese in unterschiedlicher Abstufung – festgelegt werden können. Auch hier bedienen wir uns des Verfahrens der Gruppierung und fassen IT-Systeme mit gleichen Sicherheitszielen zusammen. Solche Gruppen nennen wir *System-Objekte*.

System-Sicherheit

Wir nennen ein IT-System bzw. ein System-Objekt *sicher,* wenn

- die Sicherheitsziele System-Integrität, System-Verfügbarkeit und Vermeidung von System-Missbrauch in der gewünschten Zusammenstellung und Abstufung erreicht und aufrechterhalten werden und
- die Datensicherheit der mit dem System(-Objekt) verarbeiteten Daten im Sinne unserer früheren Definition gegeben ist.

Diese Definition ist so gestaltet, dass ein sicheres IT-System stets auch die Sicherheit der verarbeiteten Daten gewährleistet – aber natürlich gilt nicht die Umkehrung!

Die Definition von System-Sicherheit lässt sich beinahe wortgleich auf einen IT-Verbund und IV-Systeme übertragen. Die System-Integrität eines IV-Systems wäre z. B. verletzt, wenn durch Manipulation einer Überwachungskamera für die Zutrittskontrolle deren Funktion unzulässig geändert würde. Die Kamera ist hier nicht Bestandteil des IT-Systems, wohl aber des IV-Systems, und zwar in der „Abteilung" Infrastruktur.

Anmerkung: Im Zusammenhang mit der Integrität eines IT-Systems begegnen wir dem eher grundsätzlichen Problem, die beabsichtigte oder zugesicherte Funktion eines komplexen IT-Systems überhaupt so *beschreiben* zu können, dass sich die Frage nach dem korrekten Ablauf sinnvoll beantworten lässt – womit wir insbesondere beim Thema „korrekte Software" angelangt sind.

Inkorrektheit von Software

Vor allem im Bereich der *Safety* – vereinfacht: Schutz von Personen vor Maschinen – ist es üblich, die Inkorrektheit von Software als eine Bedrohung für Personen aufzufassen. Um die Konfusion komplett zu machen, wird dabei sogar von der *Integrität der Software* im Sinne des korrekten Funktionierens gesprochen.

Im Bereich der *Informationssicherheit* (*IT Security*) – sehr vereinfacht: Schutz von Informationen und Daten vor Personen – treffen wir auf dieses Problem immer dann, wenn es um die *korrekte Realisierung von Sicherheitsfunktionen* in Hard- und Software geht. Beispielsweise würde eine Zugriffskontrolle keinen Sinn machen, wenn sie nicht nachweisbar korrekt funktioniert.

Die Korrektheit nachzuweisen ist ein Ziel von Evaluierungen und Zertifizierungen nach internationalen Standards. Die Möglichkeit, Software in manipulativer Absicht inkorrekt zu machen – auch z. B. das Einfügen von undokumentierten Nebenfunktionen –, wird dabei zwar als Bedrohung aufgefasst, aber unter anderen Überschriften eingeordnet:

- Geschieht dies bei der *Entwicklung* von Software, handelt es sich um ein Problem der „Sicherheit in der Entwicklungsumgebung".
- Wird eine solche Manipulation bei der *Nutzung* von Software vorgenommen, geht es darum, ob die Einsatzumgebung und das IT-System selbst eine solche Manipulation verhindern können.

Diese Sachverhalte muss man berücksichtigen, wenn man zertifizierte IT-Produkte oder IT-Systeme einsetzen will.

4.3 Geschäftsprozesse

Die Integrität und die Verfügbarkeit von Geschäftsprozessen definiert man praktisch wortgleich wie bei den IT-Systemen. Betrachten wir deshalb noch zwei Sicherheitsziele, die für Geschäftsprozesse typisch und spezifisch sind.

Verbindlichkeit

Personen und Institutionen kommunizieren im Rahmen von Geschäftsprozessen miteinander. Dabei tritt ein neues Sicherheitsproblem auf: die *Verbindlichkeit* der Kommunikation. Dabei geht es darum, dass

- Kommunikationspartner ihre Identität einerseits nachweisen (*Authentizität*) und andererseits nicht bestreiten können *(Non Repudiation)*,
- Daten korrekt und zuverlässig zwischen Kommunikationspartnern übertragen werden können (*Integrität* der Daten beim Transport und *Verfügbarkeit* des Transportdienstes),
- der Empfang und das Absenden von Daten nicht geleugnet werden kann *(Non Repudiation)*.

Eine verbindliche Kommunikation zeichnet sich für jeden Partner dadurch aus, dass er sicher weiß, mit wem er es auf der anderen Seite zu tun hat, und davon ausgehen kann, dass gesendete Daten auch beim Empfänger korrekt und nachweisbar ankommen – Eigenschaften, die durch Manipulation wie auch durch technische Unzulänglichkeiten beeinträchtigt sein können.

Um den Verlust der Integrität bei der Datenübertragung und vorgetäuschte Identitäten erkennen zu können, sind als Sicherheitsmaßnahmen vor allem die elektronische Signatur mit Zertifikaten

eines Trust Centers bzw. eines Zertifizierungsdiensteanbieters[17] einsetzbar (s. Abschnitt „11.7 Elektronische Signatur“).

Mit der garantierten Zustellung und der Nichtabstreitbarkeit des Sendens und Empfangens haben wir bei der Nutzung des Internets, gelinde gesagt, ein Problem, weil dieses Netz solche Eigenschaften nicht aufweist. Ein Empfangsnachweis bei Emails kann zwar in den bekannten Mail-Systemen durch eine Empfangsquittung realisiert werden – allerdings nicht, wenn der Empfänger diese Maßnahme (gleich, aus welchen Motiven) abschaltet. Ein *beweisbares* Zustellen der Email liegt also nicht vor.

Rechtssicherheit

Bei vielen Geschäftsprozessen ist die *Rechtssicherheit* ein weiteres wichtiges Ziel: Eine gegen geltendes Recht verstoßende Datenverarbeitung könnte z. B. im Zusammenhang mit personenbezogenen Daten auftreten, etwa dann, wenn die Grundziele des Datenschutzes – die Datenvermeidung bzw. Datensparsamkeit, die Zweckbindung – missachtet werden. Ein anderes Beispiel wäre der Betrieb von öffentlichen Online-Diensten, ohne die einschlägige Gesetzgebung zu berücksichtigen. Schlussendlich muss es sich nicht immer um Gesetze handeln – auch Verträge, die mit Kunden geschlossen werden, sind unter dem Stichwort Rechtssicherheit zu betrachten.

Rechtssicherheit besteht dann, wenn alle maßgeblichen Gesetze und Verträge eingehalten werden und dies nachgewiesen werden kann.

Gruppierung zu Objekten

In aller Regel wird ein Unternehmen nicht nur *einen* Geschäftsprozess betreiben, womit sich wieder die Überlegung anschließt, Geschäftsprozesse mit gleichen Sicherheitszielen zu gruppieren und in der Folge von *Prozess-Objekten* zu sprechen.

Sicherheit eines Geschäftsprozesses

Wir nennen einen Geschäftsprozess (bzw. ein Prozess-Objekt) *sicher*, wenn in der gewünschten Zusammenstellung und Abstufung jeweils

- die Sicherheitsziele Rechtssicherheit und Verbindlichkeit sowie (Prozess-) Integrität und (Prozess-)Verfügbarkeit erreicht und aufrechterhalten werden,
- die ggf. unterstützenden IT-Systeme bzw. System-Objekte sicher sind (in Sinne der früheren Definition der System-Sicherheit),

17 Im Englischen: Certification Service Provider (CSP)

– die Sicherheit der im Geschäftsprozess genutzten und verarbeiteten Daten gegeben ist[18].

Man beachte hierbei, dass diese Definition auch papiergebundene und sonstige, nicht in IT-Systemen gespeicherte Daten einschließt.

Ordnungsmäßigkeit

Ein weiteres Ziel für Geschäftsprozesse – wenn auch kein Sicherheitsziel – ist die *Ordnungsmäßigkeit*. Hierunter versteht man die Eigenschaft des Geschäftsprozesses, die beabsichtigte Leistung bzw. das erwartete Ergebnis korrekt zu liefern und dies durch Aufzeichnungen nachweisen zu können.

Es hat eben alles „seine Ordnung", wenn die zugesicherte Leistung erbracht wird und man dies auch noch nachweisen kann: Der ordnungsgemäße Geschäftsprozess „tut (nachweislich) das, was er soll". Analog definiert man die *ordnungsgemäße Datenverarbeitung*.

Es ist leicht einzusehen, dass ordnungsgemäße Geschäftsprozesse noch keine sicheren Geschäftsprozesse sein müssen – und umgekehrt ein sicherer Geschäftsprozess nicht automatisch ordnungsgemäß ist. Ein erstrebenswerter Zustand wäre es offensichtlich, wenn ein Geschäftsprozess tut, was er soll (Ordnungsmäßigkeit) – und nichts tut, was er nicht soll (Sicherheit).

Revisionsfähigkeit

Bei der Rechtssicherheit und der Ordnungsmäßigkeit stellt sich gleichermaßen das Problem der Nachweise: Nachweise führt man durch das Erstellen von aussagefähigen Aufzeichnungen. Man protokolliert bzw. sichert Beweise (Sicherheitsfunktion Protokollierung bzw. *Beweissicherung*, im Englischen: *Accounting*). Sichern heißt dabei, dass die Aufzeichnungen

– alle Informationen enthalten, die für die Beweisführung notwendig sind,
– nicht nachträglich manipuliert werden können,
– jederzeit verfügbar sind.

Unter solchen Bedingungen wird ein Geschäftsprozess *revisionsfähig*.

---

18 Soweit die Verarbeitung nur durch die unterstützenden IT-Systeme geschieht, ist diese Forderung schon in dem vorhergehenden Aufzählungspunkt enthalten (s. Begriff *Datensicherheit*).

5 Analysen

Bei den vielen unterschiedlichen Analysen, die im Rahmen des Sicherheitsprozesses zur Anwendung kommen können, verliert man schnell den Überblick – zumal es sehr unterschiedliche Betrachtungsmodelle gibt.

Falls Sie sich die Frage stellen, ob so viele Analysen notwendig sind: Unsere gesamte Sicherheitskonzeption fußt darauf, dass wir die Anforderungen und Gefahren richtig analysieren und mit den Risiken verantwortlich umgehen; diesem Punkt gebührt deshalb extreme Aufmerksamkeit und sorgfältige Vorgehensweise. Die Verantwortung für die Richtigkeit der Analysen ist nicht zu unterschätzen – es kann deshalb sinnvoll sein, diese Verantwortung zu teilen, d. h. das Vorgehen in einzelne Schritte zu zerlegen und diese jeweils durch andere Personen ausführen zu lassen.

Wir stellen drei Vorgehensmodelle vor:

- Die Methode des IT-Grundschutzes.
- Die Risikoanalyse nach ISO 13335.
- Ein Analysemodell auf der Basis der ISO 15408.

5.1 Betrachtungsmodell der ISO 27001

Der Leser wird erstaunt sein, dass in der obigen Aufzählung die ISO 27001 fehlt. Das hat seinen Grund darin, dass dieser Standard keine besondere Methode der Risikobetrachtung vorschreibt, sondern für die Begriffsbildungen auf den ISO-Guide 73 verweist, der seinerseits auch nur einige allgemeine Hinweise gibt.

Dennoch erscheint es wichtig, einige Zusammenhänge genauer zu beleuchten:

Risiko

Gemäß dem genannten ISO-Guide ist ein *Risiko* eine „Kombination“ aus

- der Wahrscheinlichkeit bzw. Häufigkeit eines schadenverursachenden Ereignisses und
- dessen Konsequenzen (also des Schadens).

Die Art der schadenverursachenden Ereignisse, die „Maßeinheit“ für den Schaden wie auch die Vorschrift zur Bildung der „Kom-

bination“ aus beiden Faktoren werden nicht weiter präzisiert, sondern sind durch den Anwender wählbar.

Ereignisse

Zu den *Ereignissen* zählen in unserem Kontext Angriffe und Manipulationen durch Personen, katastrophale Ereignisse (wie Erdbeben, Feuer, Wassereinbruch, Blitzeinschlag), aber auch Fahrlässigkeit, Fehlbedienung, Verstöße gegen Vorschriften und Gesetze.

Konsequenzen

Konsequenzen drücken sich immer in Schäden für das Unternehmen aus. Diese können ganz unterschiedlich sein: vorrangig möglicherweise finanzielle Verluste, dann aber auch Ansehensverlust, Verlust der Kreditwürdigkeit oder Qualitätsverluste.

Kombination

Kann man die Konsequenzen in Zahlen ausdrücken, wird das Risiko normalerweise als *Produkt* aus Wahrscheinlichkeit und Konsequenz (=Schadenhöhe) festgelegt.

Andere Verfahren – z. B. unterschiedliche Gewichtung von Wahrscheinlichkeit und Schadenhöhe – können ebenfalls den Vorgaben aus /ISO 73/ genügen.

Statistiken

Im Einzelfall ist besonders die Ermittlung von Wahrscheinlichkeiten ein Problem: Man kann sie aus einschlägigen Statistiken gewinnen, solange es um Elementarereignisse (Katastrophen) oder um Ausfall von Geräten geht. Für andere uns interessierende Ereignisse (z. B. Hacker-Angriffe, Insider-Manipulationen) ist man auf Schätzungen bzw. Annahmen angewiesen, deren Belastbarkeit jedoch meist sehr gering sein dürfte.

Risikoanalyse

Nun aber zu den Begriffen: Als *Risikoanalyse* wird in der ISO 2700x das Verfahren bezeichnet, mit dem man

- im ersten Schritt Risiken *identifiziert* (ermittelt, benennt, grob beschreibt) und dann
- im zweiten Schritt jeweils die Höhe des Risikos *abschätzt* oder zumindest klassifiziert.

Letzteres kann nach der oben beschriebenen Kombination aus Wahrscheinlichkeit und Konsequenz geschehen. Sofern man keine genauen Zahlen ermitteln kann, sollte man einige (wenige) grobe Risikoklassen definieren und die identifizierten Risiken in diese Klassen einsortieren.

Risikobewertung

Die Höhe des Risikos bzw. die Risikoklasse ist für sich genommen noch nicht aussagekräftig. Vielmehr muss das Risiko (die Risikoklasse) im Kontext der Geschäftstätigkeit des betreffenden Unternehmens *bewertet* werden.

Das absolute Risiko (die mittlere Schadenerwartung) – als Beispiel ein Verlust von 1 Mio. € –, mag für Unternehmen A existenzgefährdend sein, für Unternehmen B dagegen ein tolerables Risiko darstellen. Die Risikobewertung besteht also darin, die Auswirkungen auf das Unternehmen anzugeben, wenn das Risiko tatsächlich eintritt.

Der Prozess aus Risikoanalyse und Risikobewertung wird in der ISO 2700x als *Risikoeinschätzung* bezeichnet.

Die folgenden Beispiele genügen mehr oder weniger diesem vorgezeichneten Begriffsrahmen – auch wenn die Begriffsbildungen bei der betreffenden Methode oft etwas anders gestaltet sind.

5.2 Analyse nach IT-Grundschutz

Der IT-Grundschutz unterscheidet zwei Vorgehensweisen:

- die klassische „schnelle“ Methode, die für „normale“ Fälle gedacht ist und auf Analysen weitgehend verzichtet, und
- die ergänzende Sicherheitsanalyse für die Fälle, in denen hohe und sehr hohe Risiken bestehen.

Es sei darauf hingewiesen, dass die erste Alternative nur begrenzten Aussagewert hat und bestenfalls für einen ersten Einstieg geeignet ist.

Schutzbedarf

Ausgangspunkt des IT-Grundschutzes ist der so genannte *Schutzbedarf*. Wir wollen uns diesem Begriff schrittweise nähern.

Betrachten wir ein zu schützendes Objekt und ein Sicherheitsziel für dieses Objekt. Man kann nun sagen:

- Das Erreichen des Sicherheitsziels hat für das Unternehmen einen bestimmten Wert, oder
- die Verletzung des Sicherheitsziels fügt dem Unternehmen einen bestimmten Schaden zu.

Ob man nun positiv (Wert) oder negativ (Schaden) bilanziert, spielt keine Rolle. Man sollte sich jedoch der Durchgängigkeit wegen für eine Alternative entscheiden. Wir verwenden die Schadenbetrachtung.

Man beachte, dass der Schaden stets unternehmensabhängig ist, d. h. für das gleiche Objekt in Verbindung mit demselben Ziel kann bei Unternehmen A eine ganz andere Schadenhöhe in Betracht kommen als bei Unternehmen B. Damit eignet sich die Schadenhöhe als solche nicht direkt für die Ableitung von allge-

mein-verbindlichen Maßnahmen, wir können aber stattdessen die *Auswirkung* des Schadens auf das Unternehmen klassifizieren:

Die Auswirkung eines finanziellen, Image- oder sonstigen Schadens auf das Unternehmen kann

- *geringfügig* (= vernachlässigbar) oder *tolerabel* sein,
- *erheblich* sein oder gar
- das Unternehmen *existentiell* bedrohen.

Durch die Verwendung solcher Vokabeln wie „geringfügig", „tolerabel", „erheblich", „existentiell bedrohend" klassifiziert man die Schadenauswirkungen – und hat sich von der konkreten Schadenhöhe als Maßstab gelöst.

Nun haben wir das Ziel praktisch schon erreicht: Hat man beispielsweise die drei zuvor genannten Stufen von Schadenauswirkungen festgelegt, dann ordnet man diesen Stufen etwa nach dem Schema in Abbildung 9 einen „Schutzbedarf" zu:

Schadenauswirkung		Schutzbedarf[19]
Geringfügig bzw. tolerabel	→	normaler Schutzbedarf
erheblich	→	hoher Schutzbedarf
existentiell bedrohend	→	sehr hoher Schutzbedarf

Abbildung 9: Schutzbedarf beim Grundschutz

Bei der Ableitung von Maßnahmen zum Schutz bestimmter Objekte orientiert man sich am Schutzbedarf für diese Objekte, d. h. an der diesbezüglichen Auswirkung von Schäden auf das betrachtete Unternehmen.

Grundwert

Es bleibt noch anzumerken, dass der Schutzbedarf bei dem gleichen Objekt je nach Sicherheitsziel – in /BSI100-2/ als „Grundwert" bezeichnet – unterschiedlich sein kann: Es kann beispielsweise vorkommen, dass die Vertraulichkeit eines Objektes einen

19 Streng genommen müsste man den Schutzbedarf „hoch" so definieren, dass die Schadenauswirkung zwar erheblich, aber nicht mehr normal sein muss; bei „sehr hoch": existentiell bedrohend und nicht mehr nur erheblich.

sehr hohen Schutzbedarf rechtfertigt, die Verfügbarkeit aber mit „normalem“ Schutzbedarf bestens versorgt ist.

Vererbungsprinzip

Als „Objekte“ werden nach der Grundschutzmethode zunächst die dort so genannten IT-Anwendungen[20] betrachtet; diese erhalten einen Schutzbedarf zugeordnet. Danach geht es im Grunde mit dem Vererbungsprinzip weiter:

- IT-Systeme, die die IT-Anwendung unterstützen, erben deren Schutzbedarf;
- Räume, in denen diese IT-Systeme aufgestellt sind, erben den Schutzbedarf entsprechend,
- Netzwerk-Segmente und -Verbindungen erben den Schutzbedarf der von den IT-Anwendungen übertragenen Daten.

Nun dürfte man selten den Fall haben, dass nur eine einzige IT-Anwendung betrachtet wird. Was passiert, wenn mehrere IT-Anwendungen die gleiche technische Infrastruktur nutzen?

Zunächst gilt der Grundsatz „Die kritischste Anwendung bestimmt das Sicherheitsniveau“:

Maximumprinzip

Der Schutzbedarf von mehreren Anwendungen, die auf einem IT-System laufen, vererbt sich so: Der höchste vorkommende Schutzbedarf bestimmt den Schutzbedarf des IT-Systems. Analog geht man hinsichtlich der Räume und Netzwerkverbindungen vor.

Von diesem einfachen Prinzip kann es Abweichungen in zweierlei Hinsicht geben:

Kumulationseffekt

Es kann einen *Kumulationseffekt* geben, durch den der resultierende Schutzbedarf höher ist als der sich aus dem Maximumprinzip ergebende: Die Vielzahl von IT-Anwendungen, die konzentriert auf einem IT-System laufen und z. B. hohen Schutzbedarf haben, kann dazu führen, dass sich der Schutzbedarf des IT-Systems quasi potenziert und bei „sehr hoch“ landet.

Verteilungseffekt

Umgekehrt kann sich durch Verteilung des Schutzbedarfs einer IT-Anwendung auf mehrere IT-Systeme ein *Verteilungseffekt* ergeben, d. h. es wird ein geringerer Schutzbedarf angesetzt, als laut Vererbungsprinzip anzusetzen wäre.

Diese drei Regeln bilden das Grundgerüst der Feststellung des Schutzbedarfs.

---

[20] in unserem Sinne: der über IT-Systeme abgewickelte Teil von Geschäftsprozessen

Anwendbarkeit

Ist der Schutzbedarf einer IT-Anwendung höchstens „normal“, werden die Maßnahmen laut IT-Grundschutz durch das BSI als ausreichend eingeschätzt. Für einen Schutzbedarf jenseits von „normal“ wird der Hinweis gegeben,

- zunächst für alle IT-Anwendungen die passenden *allgemeingültigen* Maßnahmen aus den Maßnahmen-Katalogen /BSI-M/ auszuwählen (Bausteine gemäß „Modellierung“) und diese zu realisieren,
- eine detaillierte individuelle Sicherheitsanalyse durchzuführen und dabei höhere Risiken durch adäquate *individuelle* Maßnahmen abzudecken.

Ergänzende Sicherheitsanalyse

Der vom BSI herausgegebene Leitfaden /BSI100-3/ unterstützt bei dieser Sicherheitsanalyse:

- Dabei geht man von den zu schützenden Objekten (Anwendungen, Systeme, Netze, Räume) aus und streicht alle, bei denen als Schutzbedarf höchstens „normal“ vorkommt.
- Dann entfernt man alle Maßnahmenbausteine (aus der Modellierung), für die nach der Streichaktion aus Schritt 1 kein zu schützendes Objekt mehr vorhanden ist.
- Bei den verbleibenden Bausteinen entnimmt man den Gefährdungskatalogen /BSI-G/ die als relevant angesehenen Gefährdungen und führt für diese die ergänzende Sicherheitsanalyse durch.

Beim letzten Schritt werden zur Beurteilung von Maßnahmen ähnliche Validierungsfaktoren wie in Abschnitt 7.2 verwendet: Eignung, Zusammenwirken, Benutzerfreundlichkeit, Angemessenheit.

Zu diesem Analyseverfahren laut IT-Grundschutz hier zwei Anmerkungen:

1. Es stellt sich bei der Sicherheitsanalyse nach /BSI100-3/ die Frage, welchen Beitrag die schon realisierten *allgemeingültigen* Maßnahmen zur Reduktion der *individuellen* Risiken leisten. Diese Frage wird durch den IT-Grundschutz (leider) nicht beantwortet – ebenso wie die Frage, warum die in den Maßnahmenkatalogen aufgeführten Maßnahmen für einen Schutzbedarf „normal“ ausreichend[21] sein sollen.

[21] Aufgrund gewisser Vorgaben zur Definition eigener Maßnahmen-

2) Die Methode, den Schutzbedarf an der Schadenauswirkung zu orientieren, führt zu einer interessanten Frage, die wir an einem Beispiel erläutern: Betrachten wir ein „kleines“ Unternehmen **A**, für das ein Verlust von 10.000 € ein Schaden darstellt, dessen Bedeutung gerade noch als „normal“ eingestuft wird; als zweites betrachten wir ein Unternehmen **B**, für das die Grenze von „normal“ erst bei 10 Mio. € liegt.

Nach der Grundschutz-Methode ergibt sich für beide Unternehmen die Aussage, dass die Maßnahmen aus /BSI-M/ für den Schutzbedarf „normal“ in beiden Fällen als ausreichend erachtet werden. Sowohl **A** wie auch **B** würden die gleiche Qualität von Maßnahmen umsetzen.
Nehmen wir nun an, dass die „Analyse“ insoweit korrekt wäre, als dass bei Unternehmen **B** – ohne weitere Maßnahmen – tatsächlich Schäden in der Höhe von bis zu 10 Mio. € auftreten könnten. Dann wäre es doch sicherlich ein „gutes Geschäft“ für Unternehmen **B**, einen gewissen Prozentsatz dieser Summe in bessere bzw. stärkere Sicherheitsmaßnahmen zu investieren. Richtig angewendet würde dies zu einem realen *Return on Security Investment* (ROSI) im Sine von Verlustminderung führen. Warum sollte **B** es dann also bei den Maßnahmen für den Schutzbedarf „normal“ bewenden lassen?

Dies beiden kritischen Anmerkungen sollen nicht den Wert des IT-Grundschutzes relativieren, sondern vielmehr transparent machen, dass man den IT-Grundschutz nicht so sehr als Methode, sondern eher als umfangreiche Quelle von Gefährdungen und Maßnahmenvorschlägen betrachten sollte, deren Sinnhaftigkeit für jeden konkreten Anwendungsfall durchdacht werden muss.

Mehr-Faktoren-Modell

Die interessante Idee des Schutzbedarfs wollen wir etwas weiter entwickeln und dabei den Schutzbedarf nicht nur „Pi mal Daumen“ festlegen – in der Hoffnung, er sei „normal“. Wir fragen uns zunächst, welche Informations-, Daten-, System- und Prozess-Objekte schützenswert sind. Offensichtlich sind dies alle Objekte, für die Sicherheitsziele bestehen und für die diese Sicherheitsziele bedroht sind. Wenn z. B. aus Kundenverträgen oder anderen Vorgaben Anforderungen an die Verfügbarkeit (Si-

---

Bausteine kann man schließen, dass die in /GSHB/ aufgeführten Maßnahmen mit der ihnen eigenen Schutzwirkung eher „rückwärts“ den Schutzbedarf festlegen.

cherheitsziel!) von Daten oder Dienstleistungen gestellt werden und die Verfügbarkeit „bedroht“ ist[22], sind die Daten und Dienstleistungen offensichtlich schützenswert. Fassen wir zusammen: Ein Objekt ist dann zu schützen, wenn

– für das Objekt Sicherheitsziele existieren und
– wenn diesen Sicherheitszielen (reale) Bedrohungen gegenüberstehen.

Der Bedarf an Schutz für dieses Objekt muss sich also ausdrücken lassen durch die „Höhe“ der Sicherheitsziele und die „Qualität“ der Bedrohungen: Qualität meint hier das Schaden- bzw. Angriffspotenzial[23]. Man kann diesen beiden Faktoren Zahlen zuordnen und aus dem Produkt dieser Zahlen je Objekt und Sicherheitsziel den Bedarf an Schutz ermitteln. Beispiel:

Höhe der Anforderung:	0 (keine Anforderung) 1 (geringe Anforderung) 2 (starke Anforderung) 3 (sehr starke Anforderung)
Schaden- bzw. Angriffspotenzial:	1 (gering) 2 (mittel) 3 (hoch)

Aus diesen drei Werten berechnen wir das Produkt und erhalten als mögliches Ergebnis eine Zahl aus der folgenden Liste: 0, 1, 2, 3, 4, 6, 9. Wir teilen diese möglichen Ergebnisse z. B. in vier Klassen ein und geben diesen sprechende Namen:

0-1 (kein oder nur geringer Schutz erforderlich)

2-3 (mittlerer Schutz erforderlich)

4-6 (hoher Schutz erforderlich)

9 (sehr hoher Schutz erforderlich)

Auf diese Weise können wir für jedes Objekt und jedes Sicherheitsziel für dieses Objekt einen Schutzbedarf ermitteln, und zwar anhand von Zahlen. Dabei kommt es nicht so sehr auf die

---

22 In den allermeisten Fällen ist zumindest die *technische* Verfügbarkeit *immer* bedroht, und zwar durch technische Defekte oder durch Defizite in der Systemumgebung (Stromausfall, Versagen der Klimatisierung, etc.).

23 Schadenpotenzial für Bedrohungen vom Typ 1, Bedrohungspotential für Bedrohungen vom Typ 2, s. Abschnitt 5.4.

Zahlen selbst an, sondern darauf, dass dieses Schema *einheitlich* für alle Objekte angewandt wird. Nur so lässt sich der Schutzbedarf einheitlich und nachvollziehbar festlegen.

Dies Modell aus *zwei* Faktoren kann man um weitere Faktoren ergänzen. Es wäre z. B. für ein Dienstleistungsunternehmen denkbar und sinnvoll, als dritten Faktor den Umsatzanteil zu skalieren, der mit einem Kunden – als Eigentümer des zu schützenden Objektes – erzielt wird. Die drei Faktoren multipliziert man und teilt die möglichen Ergebnisse wieder in Klassen für den Schutzbedarf ein. Hierdurch erreicht man eine Klassifizierung des Schutzbedarfs, bei der die Objekte von Kunden mit hohem Umsatzanteil höher bewertet werden als solche mit niedrigerem Umsatzanteil – eine für Dienstleister legitime und sinnvolle Sichtweise.

5.3 Risikoanalyse nach ISO 13335-3

Eine detaillierte individuelle Risikoanalyse erfordert einen nicht unbeträchtlichen Einsatz von Ressourcen. Zur wirtschaftlich sinnvollen Gestaltung werden Risiken gemäß ISO 13335-3 in einem mehrstufigen Verfahren („Combined Approach“) ermittelt, bei dem in den ersten Stufen vereinfachte Abschätzungen – zum Beispiel mit Hilfe von „Scorecards“ – eingesetzt werden.

Mit den Scorecards werden alle Risiken abschätzt; darunter auch diejenigen, die wirtschaftlich zunächst von geringer Bedeutung sind. Nur Risiken, bei denen das erwartete Schadenausmaß eine festgelegte Höhe übersteigt, werden in einer nachfolgenden Stufe einer Detaillierung unterzogen.

Dabei wird der Prozess der Risikoanalyse in die folgenden Teilschritte strukturiert:

- Definition des Risiko-Objektes/Subjektes
- Definition der Teilrisiken
- Beschreibung der relevanten Bedrohungsszenarien mit Abschätzung des Schadensausmaßes im Eintrittsfall und der Eintrittswahrscheinlichkeit
- Aufstellen von Schwachstellen- und Maßnahmenlisten
- Ermittlung des Risikos

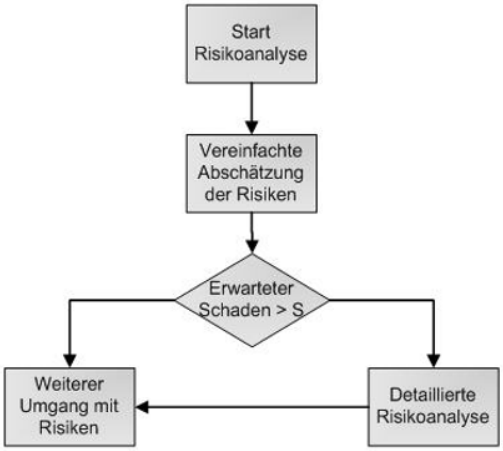

Abbildung 10: Mehrstufige Risikoanalyse

Fallbeispiel

Die vereinfachte Risikoabschätzung kann beispielsweise über die Schwere (oder auch Tiefe) der Schwachstellen gegenüber den darauf zielenden Bedrohungen vorgenommen werden. Die Eintrittswahrscheinlichkeit einer Bedrohung ist umso größer, je „schwerer" die Schwachstelle und je höher das Bedrohungspotenzial ist. Aus der nachstehenden Scorecard lässt sich ein qualitativer Wert für die Eintrittswahrscheinlichkeit ablesen.

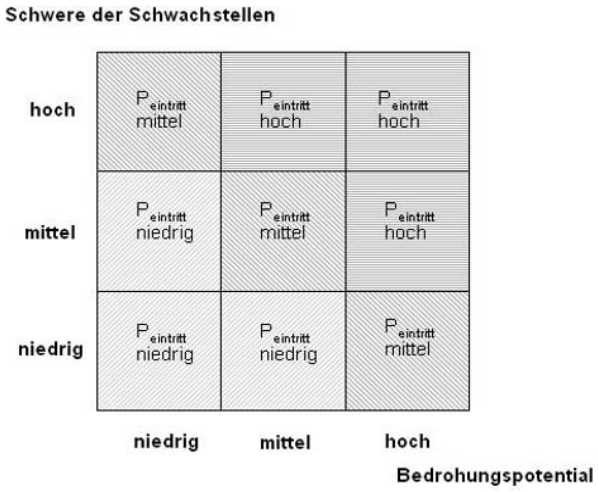

Abbildung 11: Scorecard: Eintrittswahrscheinlichkeit

Über den Wert des Risiko-Objektes und einer weiteren Scorecard erhält man einen groben Schätzwert für das mit der betrachteten Bedrohung verbundene Risiko.

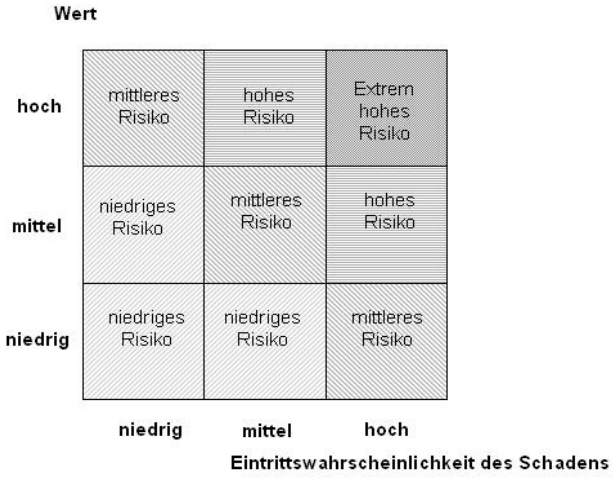

Abbildung 12: Scorecard: Risiko

Definition des Risiko-Objektes/Subjektes

Als erster Schritt der Risikoanalyse ist präzise zu definieren, für welche Objekte und/oder Subjekte (value asset) der Erwartungswert eines Schadens – nichts anderes ist ein Risiko – ermittelt werden soll. Eine möglichst genaue Eingrenzung erleichtert bzw. ermöglicht die für weitere Schritte benötigte Erhebung der Daten.

Risiko-Objekte in der IT können Infrastrukturservices und – darauf aufbauend – Kundenservices sein. Kundenservices bedienen sich meist eines oder mehreren Infrastrukturservices wie Netzwerk, Storage, Server Operating etc.

Subjekte sind agierende Personen, die Teil der Wertschöpfungskette sind; beispielsweise Administratoren, Operator usw.

Viele Risiken lassen sich zur vereinfachten weiteren Betrachtung in Teilrisiken zerlegen, die sich spezifischer auf Objekte (Infrastruktur, Prozesse, etc.) oder Subjekte beziehen.

Als nächstes sind die Bedrohungen für jedes Teilrisiko aufzulisten.

Struktur der Risikoanalyse nach ISO13335-3

Bevor wir die einzelnen Elemente und Schritte der Risikoanalyse nach ISO 13335-3 im Einzelnen erläutern, wollen wir zunächst zum besseren Verständnis die gesamte Struktur der Risikoanalyse vorstellen. Das Risiko ist der erwartete Schaden und wird von drei Variablen bestimmt:

- dem größten Schaden, der sich bei der Manifestation einer Bedrohung ergibt,
- der Wahrscheinlichkeit, mit dem diese Bedrohung und damit der Schaden eintritt und
- der für diese Bedrohung vorhandenen Ausnutzbarkeit von Schwachstellen.

Fallbeispiel

Zur Verdeutlichung des oben aufgeführten Sachverhaltes wollen wir uns als Beispiel die Bedrohung „Brand in einem UNIX-Serverraum“ ansehen. Nehmen wir an, auf den UNIX-Servern laufen sämtliche SAP-Applikationen des Unternehmens. Wir schätzen den bei einem Brand entstehenden Schaden mit Ausfall der SAP-Applikationen bis zum Wiederanlauf nach 3 Tagen auf 15 Mio. Euro (worst case).

Die Wahrscheinlichkeit für einen Brand entnehmen wir für das Gebäude geeigneten Tabellen, beispielsweise von Versicherungen, und erhalten eine Eintrittswahrscheinlichkeit von 5%.

Sicherheitsmaßnahmen haben wir in Form von Brandmeldern und Feuerlöschern im Serverraum, was den erwarteten Schaden beim Brand herabsetzt. Wir schätzen, dass die Sicherheitsmaßnahmen den Schaden um 30% reduzieren.

Allerdings haben wir die Schwachstellen, dass das Personal für den Gebrauch der Feuerlöscher keine Schulung hatte und wir seit 3 Jahren keine Übung mit Überprüfung der Brandmelder durchgeführt haben. Wir schätzen ab, dass diese Schwachstellen den möglichen Schaden wieder um 30% erhöhen. Der Schutzeffekt der Sicherheitsmaßnahmen wird so gerade wieder aufgehoben und das Risiko als Erwartungswert des Schadens ergibt sich so zu 15 Mio. x 0,05 = 750.000 Euro.

Diese drei Variablen sind zu bestimmen, beziehungsweise „praxistauglich“ abzuschätzen. Dabei geht man in der ISO 13335-3 davon aus, dass jedem Schaden eine Bedrohung vorausgeht – ein Szenario, bei dessen Realisierung sich der Schaden mit einer bestimmten Wahrscheinlichkeit einstellt. Allerdings muss das

betrachtete Risiko-Objekt, auf das die Bedrohung zielt, für diese Bedrohung exponiert sein.

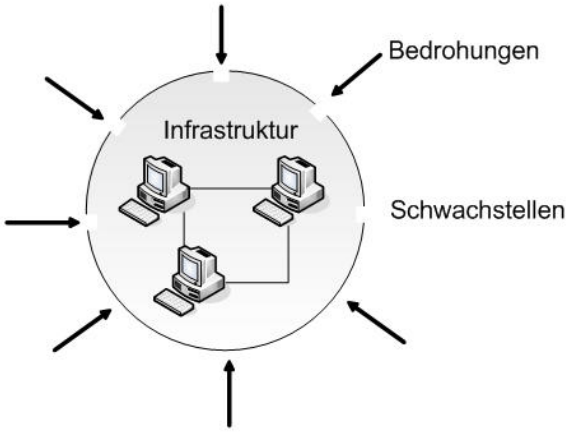

Abbildung 13: Bedrohungen bei Schwachstellen von Infrastrukturen

Fallbeispiel

Wenn kein Online Banking betrieben wird, kann ein PC-Anwender auch höchstwahrscheinlich nicht Opfer von Phishing Attacken werden. Seine Infrastruktur ist für diese Art von Bedrohung nicht exponiert.

Bei der Risikoermittlung kommt hinzu, welche Schwachstellen das Risikoobjekt aufweist, wie ernst diese Schwachstellen sind und wie gut die Sicherheitsmaßnahmen, die implementiert sind, dagegen schützen.

Praxistipp

Es gilt in diesem Kontext die einfache Faustregel: Eine Schwachstelle ist eine fehlende oder nicht funktionierende Sicherheitsmaßnahme.

Sie sehen, es gibt vielfältige Faktoren, die bei der Risikoanalyse herangezogen werden müssen. Die nachfolgende Abbildung soll die Struktur der Risikoanalyse nach ISO13335-3 verdeutlichen:

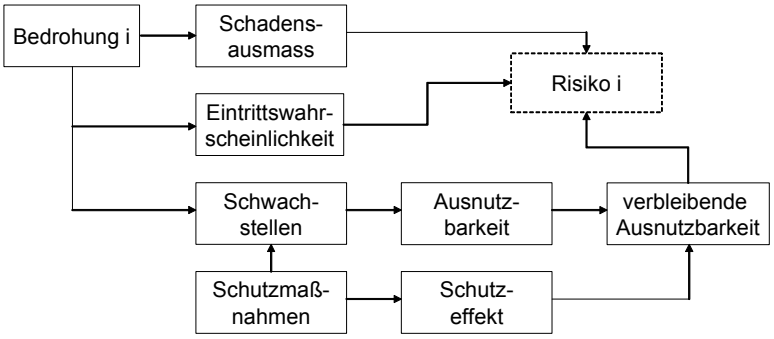

Abbildung 14: Struktur der Risikoanalyse nach ISO 13335-3

Um an die benötigten Daten zu gelangen, stehen dem IT-Risikomanager mehrere Grundmethoden zur Verfügung. In der Praxis werden oft mehrere kombiniert, zum Beispiel:

- Standardisierte Befragungen
- Prüfung entsprechender Dokumente und Unterlagen
- Betriebsbesichtigungen, interne Audits
- Zuhilfenahme interner und externer Informationsquellen

In der Praxis hat es sich als Vorteil erwiesen, standardisierte Befragungen in Form von Interviews durchzuführen.

Die standardisierte Befragung bedient sich grundsätzlich eines Fragebogens, der je nach Einsatzgebiet sehr umfangreich gehalten sein kann. Darin werden sowohl allgemeine, als auch branchen- oder systemspezifische Sachverhalte angesprochen und abgefragt.

Diese Fragebögen sind aus zwei Gründen standardisiert. Zum einen sollen die Fragen für alle Befragten einer Analyse gleich sein, zum anderen dürfen sich die Fragen bei mehrmaliger Durchführung nicht ändern. Beides bringt den Vorteil der Vergleichbarkeit.

Dabei sollte darauf geachtet werden, dass die Fragen möglichst neutral formuliert sind.

Praxistipp

Bereits einfache vom Interviewer genutzte Halbsätze könnten das Ergebnis verfälschen. Zum Beispiel: „Sie haben doch nicht etwa...“ oder „Sie werden doch bestimmt...“. Diese Art der Fragestellung impliziert eine Erwartungshaltung des Interviewers, die den Befragten möglicherweise zu einer nicht korrekten Aussage verleitet, und sollte vermieden werden. Sehr einfach kann so

etwas passieren, wenn eine qualitative Skala verwendet wird, so wandelt sich beispielsweise eine Antwort von „trifft zu“ in ein „trifft größtenteils zu“.

Der große Vorteil der standardisierten Befragung liegt in ihrer universellen Einsetzbarkeit, denn solche Fragebögen oder Interviews lassen sich in nahezu allen Branchen anwenden. Doch trägt diese Art der Risikoidentifikation neben der möglichen Subjektivität, die sich nie gänzlich ausschließen lässt, einen weiteren Nachteil in sich. Es ist nicht möglich, sämtliche Risiken, insbesondere abteilungsspezifische, durch eine standardisierte Befragung abzudecken.

Eine standardisierte Befragung kann, wenn sie selbsterklärend aufgebaut ist, auch ohne einen Interviewer ausgeführt werden. Es wird ein Fragebogen entworfen, der nach einer vorherigen telefonischen Ankündigung den betreffenden Mitarbeitern zugesendet wird. Bei dem Ausfüllen der Fragebögen besteht allerdings die Gefahr, dass sich der Befragte nur auf das schnelle Ausfüllen des Fragebogens konzentriert und seine Antworten nicht länger überdenkt oder hinterfragt. Ein Fragebogen bietet sich bei einer großen Zahl von Außenstellen an, bei denen es unwirtschaftlich wäre, Interviewer zu entsenden.

Bedrohungen

Jedes Objekt und Subjekt, für welches ein Teilrisiko ermittelt werden soll, ist Bedrohungen ausgesetzt, bei deren Manifestierung ein Schaden entsteht. Im nächsten Prozessschritt der Risikoanalyse werden für jedes Teilrisiko realistische Bedrohungen (oft auch Bedrohungsszenarien) aufgelistet. Die vorgegebenen Bedrohungskategorien und Bedrohungsbeispiele werden als Bedrohungskatalog bezeichnet und dienen dem Interviewer während der Risikoanalyse als Leitfaden. Der Erstellung dieses Risikokataloges kommt also eine wichtige Rolle zu. Diesen Risikokatalog ohne weitere Literatur neu zu erstellen ist sehr zeitaufwendig und birgt die große Gefahr, dass wichtige Punkte nicht bedacht werden. Der Katalog wäre damit unvollständig.

Im Anhang D der ISO 13335 sind einige IT-spezifische Schwachstellen aufgeführt, denen sich Bedrohungen entnehmen lassen. Diese haben sich nicht als ausreichend erwiesen, da sie nur einen beschränkten Bereich des Scopes einer IT-Risikoanalyse abdecken.

Das BSI bietet im Zusammenhang mit dem IT-Grundschutz einen sehr umfangreiche „Gefährdungskatalog“ /BSI-G/. Dieser Katalog ist in fünf Klassen eingeteilt und enthält über 300 verschiedene Gefährdungen – im Sinne der ISO 1335-3 als *Bedrohungen* zu interpretieren. Unter diesen „Bedrohungen“ sind aber Schwachstellen und „echte“ Bedrohungen stark gemischt und müssen für die weitere Verwendung sortiert werden.

Wie wir bereits wissen, reicht es nicht aus, die Bedrohungen zu identifizieren, um ein Risiko ermitteln. Es wird zusätzlich mindestens die Eintrittswahrscheinlichkeit und die zu erwartende Schadenshöhe benötigt, um mittels einer Risikoformel eine Risikohöhe zu bestimmen. Für diese Risikoanalyse werden diese beiden bisher genannten Kennzahlen jeweils zweimal erfragt – einmal, ohne dass Sicherheitsmaßnahmen getroffen sind, und ein weiteres Mal, nachdem Sicherheitsmaßnahmen etabliert worden sind. Auf diese Weise lässt sich recht einfach erkennen, wie gut und in welche Richtung die Sicherheitsmaßnahmen wirken.

Die Schwachstellen müssen explizit aufgeführt werden. Zu jeder von ihnen wird eine weitere Kennzahl namens „ease of exploitation“ erfragt. Diese wird in der ISO-Nomenklatur auch als „level of vulnerabilities“ bezeichnet. Im Deutschen bedeutet dieser Begriff soviel wie „Ausnutzbarkeit einer Schwachstelle“. Diese Erklärung erscheint jedoch bei einigen Bedrohungen, insbesondere sei hier höhere Gewalt genannt, als wenig sinnvoll. In diesen Fällen wird „ease of exploitation“ wie folgt interpretiert: „Wie einfach entwickelt sich aus dieser Schwachstelle ein ernster Schaden?“

Neben den bereits implementierten wird auch nach weiteren möglichen Sicherheitsmaßnahmen und ihrer Wirkung gefragt. Auf diese Weise werden die Verantwortlichen in der IT motiviert, über eine weitere Verbesserung der Risikosituation nachzudenken und haben gleichzeitig die Möglichkeit, ihre Vorschläge an das Management heran zu tragen. Wie den vorangegangenen Kapiteln zu entnehmen ist, muss die Geschäftsleitung das verbleibende Restrisiko durch Unterschrift akzeptieren. Der Bericht enthält auch eine Zusammenfassung von möglichen zusätzlichen Sicherheitsmaßnahmen.

Zu jedem Bedrohungsszenario sind im nächsten Schritt Kenngrößen über das Bedrohungspotenzial zu ermitteln.

Schadensausmaß (S)

Wie wir oben bereits festgestellt haben, ist jede Bedrohung – wenn sie denn eintritt – mit einem Schaden verbunden, ansonsten ist sie irrelevant und wird nicht weiter betrachtet. Als erste wichtige Kenngröße ist das *Schadensausmaß* zu ermitteln. Je nach vorliegendem Datenmaterial kann es die Festlegung des Schadensausmaßes vereinfachen, wenn zunächst der Gesamtschaden in Teilschäden zerlegt wird und später die Teilschäden aufsummiert werden. Zur Abschätzung des Schadensausmaßes lässt sich beispielsweise die nachfolgende Tabelle, die sich am Umsatz oder Budget für den betrachteten Infrastruktur- oder Kundenservice orientiert, verwenden.

Tabelle 4: Beispiel zur Abschätzung des Schadens

Schadensausmaß	Qualitativer Wert	Quantitativer Wert
Kleiner 5% vom Budget/Umsatz	niedrig	20%
Zwischen 5% und 20% vom Budget/Umsatz	mittel	40%
Zwischen 20% und 40% vom Budget/Umsatz	hoch	60%
Größer 40% vom Budget/Umsatz	sehr hoch	80%

Eintrittswahrscheinlichkeit (P)

Für jede Bedrohung ist die Eintrittswahrscheinlichkeit zu ermitteln. In den meisten Fällen kann diese nur über relative Häufigkeiten abgeschätzt werden, da es oft kein verlässliches Zahlenmaterial gibt. Ergebnis der Abschätzung ist eine reelle Zahl zwischen 0 und 1 für die Eintrittswahrscheinlichkeit. 0 bedeutet, die Bedrohung manifestiert sich nie; 1 heißt, sie tritt unmittelbar mit absoluter Sicherheit ein.

Falls wir eine qualitative Abschätzung mit einer Metrik (niedrig, mittel, hoch, sehr hoch) verwenden, ist das gleichbedeutend mit einer entsprechenden Unterteilung des [0,1] Intervalls und kann als eine Zahl abgebildet werden. Eine entsprechende Metrik kann beispielsweise wie folgt aussehen und dient zur Unterstützung der Abschätzung:

Tabelle 5: Abschätzung der Eintrittswahrscheinlichkeit

Beobachtete Häufigkeit	Qualitativer Wert	Quantitativer Wert
Einmal pro Jahr	niedrig	20%
Zweimal pro Jahr	mittel	40%
Einmal pro Monat	hoch	60%
Häufiger als einmal pro Woche	Sehr hoch	80%

Bei anderen beobachteten Häufigkeiten kann zwischen den Einträgen in der Tabelle extrapoliert werden; dabei reichen Angaben in ganzen Prozenten und in Abstufungen von 5% völlig aus. (also 5%-10%-15% usw. und nicht 17,84%).

Aufstellen von Schwachstellen/Maßnahmen-Listen

Im letzten und wichtigsten Schritt ist die Exponierung unseres betrachteten Objektes oder Subjektes zu ermitteln.

In den vorausgegangenen Schritten wurden zu jedem Objekt die Bedrohungen aufgelistet und deren Potential, nämlich Schadensausmaß und Eintrittswahrscheinlichkeit, abgeschätzt. Was zur Risikoermittlung noch fehlt, ist eine Maßzahl, die angibt, wie sehr das betrachtete Objekt oder Subjekt durch die Bedrohung verletzbar oder der Bedrohung gegenüber exponiert ist.

Die Verletzlichkeit ist unmittelbar mit der Fragestellung verknüpft, welche Schwachstellen das Objekt oder Subjekt gegenüber der Bedrohung besitzt und welche Schutzmaßnahmen bereits getroffen wurden. Erfasst man bei den Schutzmaßnahmen deren Kosten, können neben der Risikoanalyse unmittelbar Kosten-Nutzen Vergleiche erstellt werden.

Zur Ermittlung der Verletzlichkeit werden zu jeder Bedrohung Listen der Schwachstellen des Objektes oder Subjektes und der Schutzmaßnahmen erstellt. Bei den Schwachstellen wird die Ausnutzbarkeit; bei den Schutzmaßnahmen die Schutzwirkung abgeschätzt

Gibt es für eine Schwachstelle eine oder mehrere Schutzmaßnahmen, so wird deren Ausnutzbarkeit entsprechend den Schutzwirkungen vermindert. Bei mehreren Schutzmaßnahmen ist die verbleibende Ausnutzbarkeit das Minimum der einzelnen reduzierten Ausnutzbarkeiten.

Folgende Tabellen verwenden wir für die Erfassung der Ausnutzbarkeit und der Schutzwirkung:

Tabelle 6: Abschätzung der Ausnutzbarkeit

Ausnutzbarkeit von Schwachstellen	Qualitativer Wert	Quantitativer Wert
Schwachstelle ist neu und nur wenigen Experten bekannt	niedrig	20%
Schwachstelle ist neu, wird aber in Fachforen bereits erwähnt	mittel	40%
Schwachstelle ist bekannt und wird nicht nur in Fachforen erwähnt	hoch	60%
Schwachstelle ist bekannt und es ist Software zur Ausnutzung allgemein verfügbar	sehr hoch	80%

Tabelle 7: Abschätzung der Schutzwirkung von Schutzmaßnahmen

Schutzwirkung von Schutzmaßnahmen	Qualitativer Wert	Quantitativer Wert
Schutzmaßnahme reduziert geringfügig entweder das Schadensausmaß oder die Eintrittswahrscheinlichkeit	niedrig	20%
Schutzmaßnahme reduziert merklich entweder das Schadensausmaß oder die Eintrittswahrscheinlichkeit	mittel	40%
Schutzmaßnahme reduziert merklich das Schadensausmaß und die Eintrittswahrscheinlichkeit	hoch	60%
Schutzmaßnahme reduziert stark entweder das Schadensausmaß oder die Eintrittswahrscheinlichkeit	sehr hoch	80%

Bei implementierten Schutzmaßnahmen reduziert sich die Ausnutzbarkeit der Schwachstellen nach folgender Tabelle:

Tabelle 8: Abschätzung der verbleibenden Ausnutzung von Schwachstellen

	Schutzwirkung von Schutzmaßnahmen			
Ausnutzbarkeit von Schwachstellen	niedrig	mittel	hoch	Sehr hoch
niedrig	niedrig	--	--	--
mittel	niedrig	niedrig	--	--
hoch	mittel	mittel	niedrig	--
sehr hoch	hoch	hoch	mittel	niedrig

Ermittlung des Risikos

Bei qualitativ vorliegenden Werten für Schaden (s), Eintrittswahrscheinlichkeit (P) und Ausnutzbarkeit von Schwachstellen (v) lassen sich die Teilrisiken durch eine einfache Produktbildung berechnen.

Teilrisiko für die i-te Bedrohung des Schutzobjektes:

$$T_i := S_i \cdot P_i \cdot v_i$$

Die Berechnung des Gesamtrisikos aus den Einzelrisiken kann auf mehrere Arten erfolgen; wie, ist in der Risikostrategie festzulegen.

Oft wird das Gesamtrisiko Risiko R durch Mittelwertbildung über alle Teilrisiken, die einem Schutzobjekt zugeordnet werden, gebildet.

$$R := \overline{T_i}$$

Eine weitere Variante ist die Angabe des Gesamtrisikos als Summe der Einzelrisiken.

$$R := \sum_i T_i$$

Falls die Werte für Schaden, Eintrittswahrscheinlichkeit und Ausnutzbarkeit qualitativ (was meistens der Fall ist) vorliegen, erfolgt

die Abschätzung der Teilrisiken für eine Bedrohung gemäß ISO13335 nach folgender Tabelle:

Tabelle 9: Abschätzung des Risikos

Eintrittswahrscheinlichkeit →		Niedrig				Mittel				Hoch				Sehr hoch			
Ausnutzbarkeit der Schwachstellen →		N	M	H	S	N	M	H	S	N	M	H	S	N	M	H	S
Schaden	Niedrig	0	1	2	3	1	2	3	4	2	3	4	5	3	4	5	6
	Mittel	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	Hoch	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	Sehr hoch	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9

Das aus der obigen Tabelle ermittelte Risiko kann maximal die Kennzahl 9 haben, die Zuordnung zu qualitativen Werten kann aus der nachfolgenden Tabelle entnommen werden.

Tabelle 10: Zuordnung der Risikokennzahlen zu qualitativem Risiko

Risikokennzahl	0 - 1	2 - 4	5 - 7	8 - 9
Risiko	niedrig	mittel	hoch	sehr hoch
Erwartungswert des Schadens	geringer als 5% vom UB[24]	zwischen 5% und max. 20% vom UB	zwischen 20% und max. 40% vom UB	größer als 40% vom UB

5.4 Ein Ansatz auf der Basis der ISO 15408

Die Abbildung 15 zeigt die Vorgehensweise auf der Basis der ISO 15408 und die wesentlichen Abhängigkeiten zwischen den Begriffen:

[24] UB = Umsatz/Budget

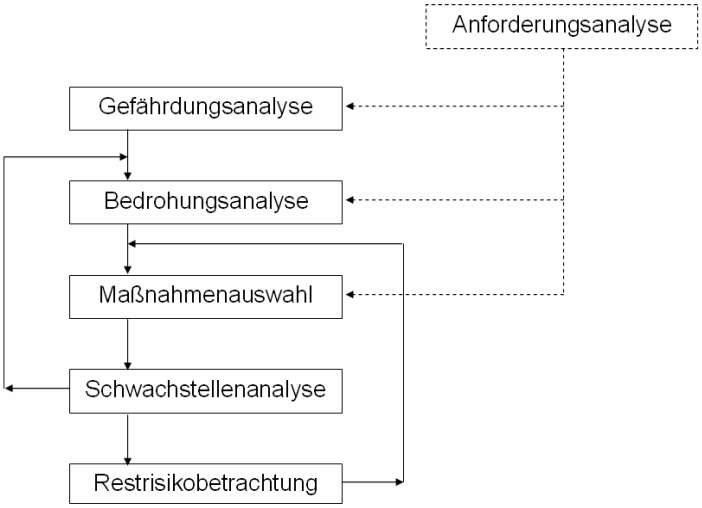

Abbildung 15: Übersicht über Analysen

Anforderungsanalyse

Die Anforderungsanalyse hat das Ziel, die Vorgaben an die IT-Sicherheit (aus Gesetzen, Verträgen, internen Richtlinien der Organisation) zu extrahieren, ihre Bedeutung für die IT-Sicherheit zu untersuchen, die so analysierten Vorgaben bzw. Anforderungen einheitlich und zusammenfassend darzustellen. Dies liefert den Input für die folgenden Analysen.

Praxistipp

Insbesondere mit Gesetzen haben wir oft das Problem, dass sie nicht *unmittelbar* erkennen lassen, was sie für Konzeption und Praxis der IT-Sicherheit bedeuten. Einen wichtigen Schritt stellt deshalb die Analyse solcher Vorgaben dar, um die Anforderungen für die IT-Sicherheit herauszufiltern. Am günstigsten ist es, dies gemeinsam mit einem Rechtsexperten zu tun, der zumindest einen groben Überblick über das Gebiet der IT-Sicherheit hat. Als Ergebnis einer solchen Analyse der Anforderungen können sich neue Gefährdungen, Bedrohungen, Sicherheitsziele, Angriffspotenziale und gar konkrete Maßnahmen ergeben.

Als Beispiel sei das deutsche Signaturgesetz /SigG/ genannt, das für die Nutzer von Signaturtechnik und Betreiber von Trust Centern Forderungen nach konkreten Maßnahmen stellt, implizit auch Gefährdungen und Bedrohungen andeutet, sogar standardmäßig ein Angriffspotenzial der Stufe „hoch“ unterstellt.

In der *Sicherheitsleitlinie* werden wir einen Abschnitt einfügen, in dem wir die zu erfüllenden Sicherheitsanforderungen aus der

Anforderungsanalyse und die bestehenden Gefährdungen zumindest summarisch, d. h. im Überblick aufführen.

Im *Sicherheitskonzept* werden wir die sich bei der Anforderungsanalyse ergebenden Gefährdungen, Bedrohungen, Sicherheitsziele, Angriffspotenziale und Maßnahmen entsprechenden Listen hinzufügen.

Entsprechend der mehrstufigen Vorgehensweise aus der Abbildung 15 werden aus Gefährdungen Bedrohungen abgeleitet; mit Sicherheitsmaßnahmen soll diesen Bedrohungen begegnet werden; allerdings können Sicherheitsmaßnahmen Schwachstellen besitzen, die wiederum Bedrohungen auslösen können; sind alle Schwachstellen betrachtet worden, können dennoch Restrisiken übrig bleiben, die unter Umständen die Wahl anderer oder ergänzender Maßnahmen erforderlich machen.

Wir greifen schon etwas vor und weisen die Schritte unseren Rollen zu: Eine Benennung der Gefährdungen eines Unternehmens könnte auf politischem Level eine Leitungsaufgabe oder Aufgabe des ISF, eine sich hieran anschließende Bedrohungsanalyse Aufgabe des Sicherheitsmanagements sein; die Analyse von Schwachstellen z. B. in der IT könnte man dort ansiedeln, wo der meiste Sachverstand vorhanden ist: bei der IT-Abteilung.

Gefährdungsanalyse

Wenn in einem Unternehmen Aussagen wie z. B. „gefährdet durch Hacker-Attacken“, „gefährdet durch Feuer“, „gefährdet durch Wettbewerber (Industriespionage)“, „gefährdet durch Innentäter“ fallen, dann wird über die *Gefährdungslage* des Unternehmens gesprochen.

Gefährdung

Diesen Aussagen ist gemein, dass sie rein qualitativ und auf einer sehr hohen Ebene Meinungen ausdrücken – vergleichbar einer politischen Einschätzung der Lage, und zwar ohne verwertbares Zahlenmaterial und ohne einzelne Abläufe konkret zu nennen. Genau das ist mit dem Begriff *Gefährdung* gemeint. Solche Aussagen sind ein wichtiger Input für das IT-Sicherheitsmanagement, da sie den Auslöser, den Gegenstand einer Gefährdung und seine Sicherheitsziele umreißen. Die in Frage kommenden *Auslöser* kann man grob einteilen in

– Elementarereignisse (Blitzeinschlag, Überschwemmung, Erdbeben usw.),

– technische Defekte und Ausfälle wie Materialermüdung bei Datenträgern, Geräteversagen; Klimatisierungs- und Stromausfall,

– Handlungen von Personen: Innentäter, Fremdpersonal z. B. für Wartung und Reinigung, Hacker, Spione.

Gegenstand von Gefährdungen sind unsere Informations- und Daten-, System- und Prozess-Objekte, für die wir ja bestimmte *Sicherheitsziele* festgelegt haben. Bei der schriftlichen Darstellung von Gefährdungen sollte man also immer die betroffenen Objekte (summarisch), das betreffende Sicherheitsziel und den Auslöser der Gefährdung benennen. Verbessern wir also die anfangs aufgezählten Wortbeiträge:

„Die System-Verfügbarkeit unserer IT-Systeme ist durch folgende Elementarereignisse (Liste…) gefährdet."

„Die Vertraulichkeit der Informationen unseres Unternehmens ist durch Wettbewerber gefährdet (Industriespionage)."

„Unsere Daten sind dem Missbrauch durch Innentäter ausgesetzt."

„Unsere Daten und Systeme sind gefährdet durch Hacker-Attacken." Meint wahrscheinlich: Alle Sicherheitsziele sind betroffen.

Nun bewertet man jede Gefährdung danach, ob

– das Unternehmen ihr *tatsächlich* ausgesetzt ist oder ob

– diese Gefährdung grundsätzlich nicht relevant ist und deshalb nicht weiter betrachtet werden muss.

Es kann sein, dass auf Leitungsebene oder im ISF Gefährdungen benannt werden, die dann aber mit dem Argument „kommt bei uns nicht vor" vom Tisch fallen. Die Verantwortung dafür liegt nach unserer Aufgabenverteilung auf dieser Ebene (Leitung oder ISF) und nicht beim Sicherheitsmanagement.

Die verbleibenden relevanten Gefährdungen *kann* man in einem zweiten Schritt nach ihren möglichen *Auswirkungen* auf das Unternehmen bewerten. Hierzu gibt man sich Stufen wie z. B. „vernachlässigbar", „beträchtliche Auswirkungen", „existenzbedrohende Auswirkungen" vor. Zu den negativen Auswirkungen können geldliche Verluste, Qualitätsverluste etwa in der Produktion, Image-Beeinträchtigung, Haftungstatbestände, nicht versicherbare Risiken u. v. m. zählen.

Gefährdungsanalyse

Das Zusammentragen der denkbaren Gefährdungen für ein Unternehmen und ihre Bewertung nach Relevanz und Auswirkung bezeichnet man als *Gefährdungsanalyse*.

Zumeist lasen sich die ermittelten Gefährdungen klassifizieren bzw. gruppieren: Eine Möglichkeit besteht darin, die Gefährdungen in das Raster „Vertraulichkeit, Verfügbarkeit und Integrität" einzusortieren. Eine andere geht von den Geschäftsprozessen des Unternehmens aus und ordnet die Gefährdungen diesen Prozessen ein.

Durch dieses Vorgehen erhält man einen zusammenfassenden Überblick über die eventuell längliche Liste der Einzelgefährdungen.

Sicherheitsleitlinie

Dieser zusammenfassende Überblick hat einen guten Platz in der Sicherheitsleitlinie, in der das Unternehmen seine Grundsätze der Sicherheit schriftlich festhält und diese u. a. mit der Gefährdungslage begründet[25]. Die Erstellung einer Sicherheitsleitlinie behandeln wir in Kapitel 6. Will man so nicht vorgehen, kann die Gefährdungsanalyse auch Bestandteil des Sicherheitskonzeptes sein – dann liegt die Verantwortung allerdings wieder allein beim Sicherheitsmanagement.

Bedrohungsanalyse

Bedrohung

Zu jeder Gefährdung gehört

- ein Verursacher oder Auslöser,
- ein der Gefährdung ausgesetztes Informations-, Daten-, System- oder Prozess-Objekt und
- mindestens ein durch die Gefährdung beeinträchtigtes Sicherheitsziel für dieses Objekt[26].

---

25 Andere Begründungen können sich aus gesetzlichen Auflagen oder aus Verträgen mit Kunden ergeben. Weitere Grundsätze werden oft auch abgeleitet aus der Forderung nach administrativer und technischer Interoperabilität (etwa in großen Konzernen mit vielen Tochterunternehmen): Man schreibt z. B. einheitliche Verschlüsselungsverfahren vor.

26 Gefährdungen, die kein Sicherheitsziel verletzten, sind keine Gefährdungen.

Jedoch liefert uns die Gefährdungsanalyse nicht automatisch den genauen Ablauf, wie aus einer Gefährdung ein Schaden entstehen kann.

Bedrohungsanalyse

Genau dies ist Aufgabe der *Bedrohungsanalyse*: Hiermit werden für jede Gefährdung alle denkbaren Abläufe und Ereignisse ermittelt, durch die diese Gefährdung Realität werden kann.

Beispiele:

1) Bei der Gefährdung „Die System-Verfügbarkeit unserer IT-Systeme ist durch Elementarereignisse gefährdet“ würde man für die IT-Systeme die möglichen Elementarereignisse durchspielen: Ausbruch eines Brandes, Blitzeinschlag, Wassereinbruch, Erdbeben, usw. und die Auswirkungen benennen.

2) Um die Gefährdung „Die Vertraulichkeit der Informationen unseres Unternehmens ist durch Wettbewerber gefährdet (Industriespionage)“ zu behandeln, würde man für die betreffenden Informationen zunächst feststellen, wo sie vorhanden bzw. gespeichert sind, um dann mögliche Wege zu ermitteln, wie Wettbewerber an diese Informationen herankommen können.

Grundsätzlich gibt es dabei zwei Methoden:

Methode 1: Bei der Bedrohungsanalyse lässt man eventuell schon vorhandene Sicherheitsmaßnahmen *zunächst unberücksichtigt*. Sie werden erst in einem späteren Schritt den Bedrohungen zugeordnet.

Methode 2: Eventuell schon vorhandene Sicherheitsmaßnahmen werden *bereits hier berücksichtigt* und dahingehend bewertet, ob sie der Bedrohung ausreichend widerstehen können. Ist dies nicht oder nur beschränkt der Fall, muss man später nachbessern.

Typ 1 und Typ 2

Unabhängig von dieser Einteilung diskutieren wir im Folgenden zwei grundsätzlich verschiedene Arten von Bedrohungen und Risiken, die wir kurz mit *Typ 1* bzw. *Typ 2* bezeichnen.

>> Bedrohungen und Risiken vom Typ 1

Häufigkeit

Bedrohungen vom **Typ 1** begegnen uns in Form eher zufälliger Ereignisse wie

- technischer Defekte (Materialermüdung, Abnutzung,…),
- Ausfällen bei Versorgungen (Strom, Klimatisierung,…),
- Elementarereignissen (Erdbeben, Blitzeinschlag,…),

wodurch Sicherheitsziele für Objekte beeinträchtigt werden können. Wir charakterisieren diese Bedrohungen durch ihre *Eintrittswahrscheinlichkeit*[27] oder *Häufigkeit*, für die wir meist relativ zuverlässige Statistiken haben oder uns verschaffen können. Diese Zahlen sind selten unternehmensspezifisch.

Risiko Typ 1

Ermittelt man noch die *Höhe des Schadens* pro Schadenfall und berechnet das Produkt aus Schadenhäufigkeit und Schadenhöhe, so erhält man den „erwarteten Schaden" für die betrachtete Bedrohung. Der „erwartete Schaden" ist gleichbedeutend mit dem *Risiko* für das Unternehmen und ist die Motivation für Gegenmaßnahmen. Das Risiko ist in aller Regel eine unternehmensspezifische Größe, da die Schadenhöhe unternehmensabhängig sein dürfte. Zur Bewertung eines Risikos verwendet man häufig ein Schema, wie es in der Abbildung 16 dargestellt ist.

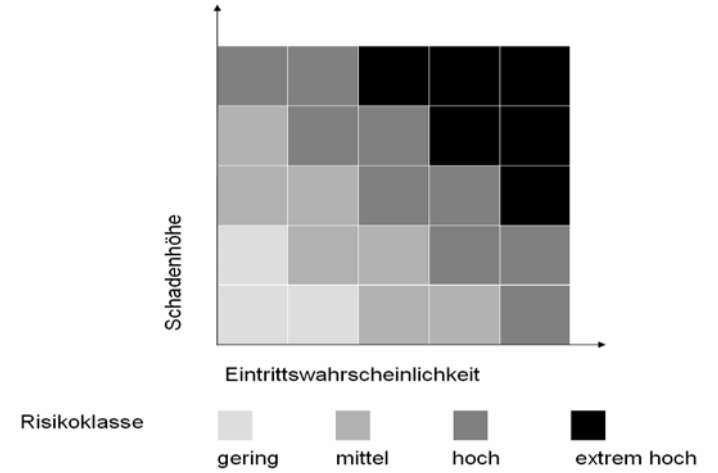

Abbildung 16: Risikoklassen für Typ 1

Für die Eintrittswahrscheinlichkeit und die Schadenhöhe einer Bedrohung sind in der Abbildung je 5 Stufen verwendet worden – man kann dies natürlich ändern; die Anzahl der Stufen für beide Parameter muss außerdem nicht gleich sein. Welche Grenzwerte bei der Schadenhöhe für die einzelnen Stufen maßgebend sind, wird individuell festgelegt. Als Beispiel könnte sich

27 Für technische Defekte bei Geräten kann man z. B. die bekannte MTBF (Mean Time between Failure) nutzen, die für viele Geräte durch die Hersteller angegeben wird.

für ein bestimmtes Unternehmen die folgende Zuordnung ergeben:

Klasse 1: Schadenhöhe < 1.000 €

Klasse 2: Schadenhöhe 1.000 – 10.000 €

Klasse 3: Schadenhöhe 10.000 – 100.000 €

Klasse 4: Schadenhöhe > 100.000 €

Es sind auch eher „weiche" Klassen definierbar wie „geringer Schaden", „tolerierbarer Schaden", „erheblicher Schaden", usw. Dies trägt dem Umstand Rechnung, dass eine rein monetäre Schadenbetrachtung zu kurz greifen kann, da andere *Schadenkategorien* existieren wie etwa Image- bzw. Vertrauensverlust und gesetzwidriges Handeln. Allerdings können sich diese Schadenkategorien letztendlich auch in Umsatzverlust auswirken, d. h. sie sind zumindest monetär *bewertbar*.

Bei der Eintrittwahrscheinlichkeit könnte man ebenfalls Zahlenbereiche angeben oder „weiche Klassen" wie „nie", „selten", „häufig", „sehr häufig" verwenden.

Die Schlussfolgerungen aus der Analyse mit einer solchen Abbildung sind

- einerseits *Prioritäten* bei der Behandlung der Risiken: die extrem hohen Risiken zuerst, dann die hohen Risiken, usw.,
- andererseits eine Begründung für die *Angemessenheit und Wirtschaftlichkeit* von Investitionen in Sicherheitsmaßnahmen.

Restrisiko Typ 1

Durch Sicherheitsmaßnahmen können wir ein Risiko reduzieren, indem wir den Schaden reduzieren oder die Eintrittswahrscheinlichkeit beeinflussen. Welche Risikoreduktion wir durch die Maßnahmen auch immer erreichen – ein Rest wird bleiben: das *Restrisiko*. Restrisiken für Bedrohungen vom Typ 1 sind typischerweise versicherungsfähig.

Ein weiterer Aspekt, der hier betrachtet werden muss, ist die Wirtschaftlichkeit: Wir müssen bei der Maßnahmenauswahl darauf achten, dass die Kosten für die Maßnahmen geringer sind als die damit erreichte Verringerung des erwarteten Schadens – andernfalls hätten wir das Gebot der *Wirtschaftlichkeit* verletzt (s. Abschnitt „7.2 Validierung von Maßnahmen").

Gesamtrisiko

Addiert man die Risiken (bzw. Restrisiken) aus allen ermittelten Bedrohungen, so erhält man das Gesamtrisiko (bzw. das vollständige Restrisiko) für das Unternehmen.

>> Bedrohungen und Risiken vom Typ 2

Beim Typ 1 haben wir absichtliche bzw. vorsätzliche Handlungen von Personen außen vor gelassen. Der Grund ist, dass uns in aller Regel keine verlässlichen Statistiken über die Eintrittswahrscheinlichkeit solcher Angriffe vorliegen, d. h. wir können das Schadenpotenzial nicht bestimmen – wohl aber den jeweils entstehenden Schaden.

Angriff

Absichtliche bzw. vorsätzliche Handlungen von Personen nennen wir *Angriffe*.

Angriffe können zudem so vielfältig, raffiniert und in einem gewissen Sinne „genial" sein, dass eine rein statistische Bewertung nach der Häufigkeit wenig Relevanz hat. Angriffe, für die wir keine verlässlichen Statistiken haben, ordnen wir der zweiten Klasse von Bedrohungen (**Typ 2**) zu.

Bewertungsfaktoren

Damit ein solcher Angriff erfolgreich ausgeführt werden kann, benötigen die Täter

- technische oder andere *Fachkenntnisse*,
- *Ressourcen* wie z. B. die für den Angriff benötigte Zeit sowie erforderliche Spezialwerkzeuge, und
- eine sich bietende *Gelegenheit*: Kenntnis über besondere Umstände, Zuarbeit von Unternehmensangehörigen.

Beispiel: Einfachste Türschlösser lassen sich mit einem gebogenen festen Draht („Dietrich") in wenigen Augenblicken auch durch einen Laien öffnen, sofern er diesen Angriff irgendwo mal gesehen hat. Zeit und Kenntnisse für ein erfolgreiches Knacken eines solchen Schlosses sind also als gering einzustufen, echte Spezialwerkzeuge werden nicht benötigt. Man benötigt natürlich freien Zugang zu der entsprechenden Tür – also die Gelegenheit zum Einbruch.

Komplexere Schlösser mit einem Schließzylinder und Zuhaltungen bedürfen schon gewisser Spezialwerkzeuge und eines versierten Angreifers, um erfolgreich geknackt zu werden. Je nach Situation wird auch erheblich mehr an Zeit benötigt.

Gute Tresorschlösser zu öffnen, braucht dagegen Zeit, Spezialwerkzeuge und einschlägige technische Fachkenntnisse – wenn es überhaupt möglich ist. Darüber hinaus ist man auf die Mitarbeit einer Person aus dem betreffenden Unternehmen angewiesen, die einem Informationen über den Typ des Tresors und die Zugangsmöglichkeiten verschafft.

Man erkennt an den Beispielen, wie sich die zu Anfang genannten Bewertungsfaktoren Fachkenntnisse, Ressourcen und Gelegenheit quasi „aufschaukeln“ und jeweils die für einen erfolgreichen Angriff benötigten Voraussetzungen ergeben. Nun wird man einwenden, dass dies eine nette Überlegung ist – kann man dies aber auch in „Zahlen“ fassen?

Angriffspotenzial

In /ITSEM/ findet man eine Klassifikation des *Angriffspotenzials*, die auf den genannten Bewertungsfaktoren beruht. Danach werden drei Stufen „niedrig“, „mittel“ und „hoch“ vorgeschlagen. Durch Auswerten der obigen Faktoren anhand von Tabellen kann man für jede Tätergruppe eine dieser drei Stufen festlegen.

Mechanismenstärke

Sicherheits- bzw. Abwehrmaßnahmen für Bedrohungen vom Typ 2 kann man danach bewerten, welches Angriffspotenzial gerade noch abgewehrt wird. Dieser „Mindestwert“ wird *Mechanismenstärke* der Maßnahme genannt.

Der geschilderte Sachverhalt wird durch die Abbildung 17 visualisiert: Für das zu schützende Objekt (Schatzkiste) deutet die Dicke des Rings die Mechanismenstärke der Sicherheitsmaßnahmen an, während die Länge des Nagels das Angriffspotenzial eines Täters angibt. Die Frage, ob Angriffe abgewehrt werden können, ist ausschließlich eine Frage der Balance zwischen Angriffspotenzial und Mechanismenstärke. Insofern ist für Bedrohungen vom Typ 2 eine Schadenermittlung obsolet.

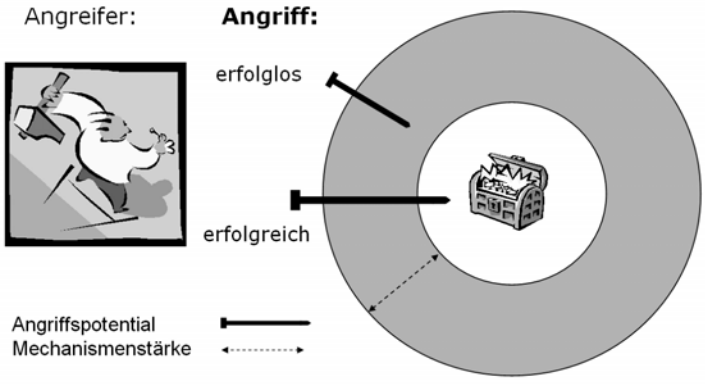

Abbildung 17: Bedrohungsanalyse vom Typ 2

Plausibilität

Nicht jeder potenzielle Täter, der ein ausreichendes Angriffspotenzial besitzt, wird aber allein deshalb einen Erfolg versprechenden Angriff auf ein Objekt tatsächlich durchführen. Beson-

ders eklatant wird dieses Problem bei den eigenen Mitarbeitern: Wenn alle Mitarbeiter – aus welchen Gründen auch immer – als vertrauenswürdig gelten, kann man trotz möglicherweise hohen Angriffspotenzials Bedrohungen durch „Innentäter" für bestimmte Objekte möglicherweise ausschließen. Man muss also das Angriffspotenzial mit einer Bewertung der *Plausibilität* eines Angriffs verbinden. Dies hat nichts mit der Eintrittswahrscheinlichkeit zu tun, denn die Plausibilität ist keine Frage der Häufigkeit.

Anmerkung: Angaben zur Mechanismenstärke von technischen Sicherheitsmaßnahmen findet man in den Zertifizierungsreports von IT-Produkten, die nach /ITSEC/ oder /CC/ zertifiziert worden sind. Wir können damit solche Bewertungen später im Sicherheitskonzept bei der Auswahl von Maßnahmen bzw. Produkten sehr gut verwenden.

5.5 Ergänzendes zur Schwachstellenanalyse

Uns ist hinlänglich bekannt, dass im Grunde jede Maßnahme Schwachstellen aufweist. Dies gilt nicht nur für technische Sicherheitsmaßnahmen, sondern z. B. auch für organisatorische Maßnahmen, an deren Ausführung bzw. Beachtung Menschen beteiligt sind.

Was ist eine Schwachstelle? Das typische Verständnis dieses Begriffes liefert die folgende Aussage:

Schwachstelle

Eine *Schwachstelle* in einer Sicherheitsmaßnahme ist ein Defizit in den Prinzipien oder der Umsetzung der Maßnahme, durch das ein erfolgreicher Angriff möglich wird.

Wie kommt es zu solchen Schwachstellen? Sie können *operativ* oder *konstruktiv* bedingt sein.

Operative Schwachstellen

Bei Schwachstellen operativer Natur liegen die Mängel in der *Anwendung* der Maßnahme. Ursachen hierfür können z. B.

- die fehlerhafte Installation bzw. Konfiguration bei Systemen,
- die fehlerhafte Umsetzung von Maßnahmen,
- der fahrlässige Umgang mit Maßnahmen,
- die mangelnde Praktikabilität von Maßnahmen (s. Abschnitt „7.2 Validierung von Maßnahmen") sein.

Fahrlässigkeit

Fahrlässige Handlungen von Befugten sind ein diffiziles Thema: Sie sind in der bisherigen Systematik der Bedrohungen weder bei Typ 1 noch bei Typ 2 einsortiert worden, da sie nicht mit Elementarereignissen, Defekten, Ausfällen und auch nicht mit

bewussten Angriffen gleichzusetzen sind: Fahrlässigkeit liegt vor, wenn sich jemand nicht präzise an Vorgaben und Regeln hält, und zwar weil er nicht „daran gedacht hat“, weil es ihm in der besonderen Situation als unwichtig erschien, ggf. aus Desinteresse, wegen Zeitdrucks oder auch deshalb, weil die Vorgaben unüberschaubar sind. Wir wollen hier nicht in die Diskussion über den *Grad* der Fahrlässigkeit („einfache“ bis „grobe“) einsteigen. Vielmehr sei an dieser Stelle vermerkt, dass man der Schwachstelle „Mensch“

- durch stärkere Awareness-Maßnahmen (s. Abschnitt 2.3 zu Sensibilisierung, Schulung und Training),
- durch intensivere Überprüfungen (s. Abschnitt 14.1) und letztlich
- (wenn nichts mehr hilft:) durch entsprechende Sanktionen begegnen kann.

Konstruktive Schwachstellen

Konstruktive Schwachstellen findet man bei fast allen Maßnahmen, insbesondere bei den Sicherheitsvorkehrungen in IT-Systemen. Die Liste bei den heute bekannten Betriebssystemen ist meist schon lang und wird immer länger. Wichtig ist, möglichst *frühzeitig* verlässliche Informationen über solche Schwachstellen zu bekommen.

CERT-Dienste

Hierzu sei dringend angeraten, sich einschlägiger Informationsdienste[28] zu bedienen, die Schwachstellen-Informationen, Risikoeinschätzungen und Vorschläge zur Behebung der Schwachstellen liefern. Zusätzlich werden oft auch Mehrwertdienste wie z. B. Seminare, Analystentage, Ansprechpartner bei Notfällen angeboten.

Es kommt aber durchaus vor, dass man mit gewissen Schwachstellen leben muss, weil es kurzfristig nicht möglich ist, sie zu beheben. Erst mit größerem zeitlichem Verzug werden ggf. von den Herstellern der Systeme entsprechende Updates angeboten, die das Problem lösen sollen – und hoffentlich nicht neue „Löcher“ aufreißen.

Schwachstellen haben leider die unangenehme Eigenschaft, sich nicht zum Zeitpunkt ihrer Entstehung, sondern erst nach einiger Zeit zu „enttarnen“. Solange man Schwachstellen aber nicht kennt, kann man auch keine spezifischen Gegenmaßnahmen

[28] Beispiele: www.mcert.de, www.cert.dfn.de, www.dcert.de, www.bsi.bund.de/certbund/.

treffen. Es bleibt dann nur die Hoffnung, dass das Gesamtpaket aller Sicherheitsmaßnahmen ein gewisses Maß an Schutz auch gegen unbekannte Schwachstellen bietet – diese Hoffnung ist aber sehr häufig unbegründet.

Ausnutzen von Schwachstellen

Schwachstellen werden erst dann zum Problem, wenn sie durch Angreifer ausgenutzt werden. In diesem Fall *können* Sicherheitsziele des Unternehmens beeinträchtigt werden – dies ist aber nicht zwingend der Fall. So kann beispielsweise eine „Denial of Service" Attacke, die aufgrund einer Schwachstelle in einem IT-System möglich ist, die Verfügbarkeit des IT-Systems stark beeinträchtigen. Dies wäre allerdings kein Sicherheitsproblem, wenn die Verfügbarkeit des IT-Systems in den Sicherheitszielen gar nicht vorkommt, der Fokus vielleicht mehr auf der Vertraulichkeit von Daten liegt.

Schwachstellenanalyse

In der Schwachstellenanalyse muss folglich jede Schwachstelle dahingehend untersucht werden,

- ob sie durch einen Angreifer prinzipiell ausnutzbar ist,
- ob ein erfolgreiches Ausnutzen der Schwachstelle den Sicherheitszielen des Unternehmens zuwider läuft,
- welches Angriffspotenzial zum Ausnutzen der Schwachstelle erforderlich ist.

Die Fragen sind in der genannten Reihenfolge zu durchlaufen.

- Ist die Schwachstelle prinzipiell *nicht* ausnutzbar – z. B. weil hierfür Zugang zu einem System erforderlich ist, der aber anderweitig ausreichend abgesichert ist –, kann die Schwachstelle ignoriert werden.
- Kann durch Ausnutzen der Schwachstelle *kein* Sicherheitsziel des Unternehmens beeinträchtigt werden, kann die Schwachstelle ignoriert werden.

Sind beide Fragen jedoch mit ja beantwortet worden, bleibt zu prüfen, ob die bei der Bedrohungsanalyse betrachteten Tätergruppen das notwendige Angriffspotenzial besitzen, um die Schwachstelle ausnutzen zu können: Hierzu mögen detaillierte Kenntnisse und Ressourcen erforderlich sein, die unsere Täter vielleicht nicht aufweisen.

- Reicht das Angriffspotenzial unserer Täter *nicht* aus, um die Schwachstelle auszunutzen, kann sie ignoriert werden.

Manche Schwachstelle wird in die Kategorie „ignorieren“ fallen. Wie geht man mit den verbleibenden um? Es gibt drei *prinzipielle* Alternativen:

- Man nimmt die Schwachstelle und das daraus resultierende Risiko in Kauf.
- Man kompensiert die Schwachstelle durch zusätzliche Maßnahmen.
- Man behebt das Problem durch einen Wechsel der Maßnahme oder des Systems.

Diese Ausführungen beziehen sich auf operative wie konstruktive Schwachstellen. Das Austauschen oder Kompensieren muss natürlich so erfolgen, dass im Ergebnis die vorgesehene Schadenreduktion (Typ 1) bzw. die vorgesehene Mechanismenstärke (Typ 2) erreicht wird.

Wir fassen zusammen: Aus operativen und konstruktiven Schwachstellen *können* Bedrohungen unserer Sicherheitsziele resultieren. Mit der Schwachstellenanalyse bewerten wir Schwachstellen dahingehend, ob sie relevant, ausnutzbar, kompensierbar sind.

5.6 Umgang mit dem Restrisiko

Wie geht man mit Restrisiken um? Hierfür gibt es grundsätzlich folgende Alternativen:

- das Restrisiko akzeptieren,
- das Restrisiko versichern, falls dies möglich ist,
- das Restrisiko verlagern, indem man besonders risikoträchtige Prozess-Anteile z. B. an Dienstleister auslagert,
- das Restrisiko in weiteren Schritten reduzieren, indem man erneut in das Sicherheitskonzept einsteigt und wirksamere Maßnahmen vorsieht – was in der Regel auch höhere Kosten bedeutet.

Zur Verlagerung des Restrisikos sei angemerkt, dass die Verantwortung für die Unternehmensprozesse und Daten grundsätzlich beim Unternehmen selbst verbleibt. Jedoch kann es eine interessante Alternative sein, bestimmte Verarbeitungen auszulagern – nicht nur unter Kostengesichtspunkten, sondern auch aus Sicht der Sicherheit: Beispielsweise können Dienstleistungsrechenzentren ein Sicherheitsniveau etablieren, das ein Unternehmen nur zu exorbitanten Kosten erreichen könnte.

6 Die Sicherheitsleitlinie

Sicherheit ist immer eine *dokumentierte* Sicherheit, d. h. es sind alle Überlegungen schriftlich festzuhalten, um eine jederzeit nachvollziehbare Grundlage zu schaffen. Sicherheit, die nur in den Köpfen der Beteiligten existiert, ist nicht analysierbar, nicht nachvollziehbar und nicht nachweisbar – und somit wertlos. Wir behandeln in diesem Abschnitt die (IT-)*Sicherheitsleitlinie*, die gelegentlich auch (IT-)*Sicherheitsleitlinie* genannt wird.

6.1 Inhalte der Sicherheitsleitlinie

Mit der Sicherheitsleitlinie gibt die Unternehmensleitung eine Grundsatz-Erklärung zur IT-Sicherheit ab und legt dabei fest,

- für welchen Bereich bzw. welche Geschäftsprozesse des Unternehmens die Sicherheitsleitlinie gilt (Geltungsbereich),
- warum IT-Sicherheit hierfür wichtig ist,
- ggf. welche (summarisch dargestellten) Gefährdungen für den Geltungsbereich bestehen,
- welche „sonstigen" Vorgaben in punkto Sicherheit einzuhalten sind,
- wie die Sicherheit organisiert werden soll (optionaler Gliederungspunkt),
- dass alle Mitarbeiter des Unternehmens verpflichtet sind, die Sicherheitsleitlinie zu beachten und einzuhalten (optionaler Gliederungspunkt).

Wir behandeln die einzelnen Gliederungspunkte nun etwas ausführlicher.

Einleitung

In einem einleitenden Absatz sollte

- das Unternehmen benannt werden,
- sein Geschäftszweck kurz charakterisiert werden sowie
- in groben Zügen die Organisation dargestellt werden und
- ggf. die Standorte des Unternehmens aufgezählt werden.

1. Anwendungsbereich

Als Anwendungsbereich einer Sicherheitsleitlinie kommen beispielsweise in Frage:

- bestimmte Organisationseinheiten oder das gesamte Unternehmen,
- ein Geschäftsprozess oder mehrere, ggf. alle Geschäftsprozesse eines Unternehmens,
- einzelne Standorte eines Unternehmens,
- die IT-Nutzung im Unternehmen generell,
- die Ressource „Information" des Unternehmens insgesamt.

In den letzten beiden Fällen spricht man genauer von der „IT-Sicherheitsleitlinie" und der „Informationsschutz-Leitlinie". Bei letzterer geht es um *alle* Informationen des Unternehmens, während bei der IT-Sicherheitsleitlinie die elektronisch zu verarbeitenden Daten im Mittelpunkt stehen.

Mit der Darstellung des Anwendungsbereichs wird meist auch die Entscheidung vorweggenommen, ob es später beim Sicherheitskonzept um die Sicherheit der IT und der Netze (klassische IT-Sicherheit) oder um die Sicherheit der Geschäftsprozesse geht (moderner Ansatz).

2. Bedeutung der Sicherheit

Bei der Frage nach der Bedeutung der Sicherheit für den Anwendungsbereich ist darzustellen, welchen „Wert" der Anwendungsbereich und seine Sicherheit für das Unternehmen haben: Wie weit hängt das Unternehmen beispielsweise von der einwandfreien, verlustfreien Funktion eines Geschäftsprozesses ab? Hängt das Image des Unternehmens von der IT-Sicherheit ab? Welche Auswirkungen könnten Sicherheitsvorfälle auf die Geschäftstätigkeit und das Image haben? Hier werden keine Zahlen erwartet, sondern qualitative Einschätzungen.

3. Gefährdungslage

Für den Anwendungsbereich kann man weiterhin darlegen, welche Gefährdungslage besteht. Hier reichen „politische" Aussagen: Wir haben dieses Thema bereits in dem entsprechenden Abschnitt „Gefährdungsanalyse" in 5.4 behandelt. Die Aussagen der Gefährdungsanalyse sind der Input für die später im Rahmen des Sicherheitskonzeptes durchzuführende Bedrohungsanalyse.

4. Weitere Vorgaben

Für das Sicherheitskonzept und die dort zu planenden Maßnahmen sind neben den Gefährdungen auch andere Vorgaben in Betracht zu ziehen, aus denen sich Anforderungen an die Sicherheit ableiten lassen:

- Es sind gesetzliche Bestimmungen einzuhalten.

Hierunter fallen z. B. die Datenschutzgesetze (BDSG und Länder-Gesetze), das Telekommunikationsgesetz (TKG), das Signatur-

gesetz (SigG). Weiterhin können sich Vorgaben für die IT-Sicherheit aus den *Grundsätzen ordnungsgemäßer Buchführung*, aus der Umsatzsteuerrichtlinie – etwa für das Gebiet der elektronischen Rechnungsstellung, aus Regelungen über Aufbewahrungsfristen (hier von Daten bzw. Dokumenten) – ergeben. Grundsätzlich fordert z. B. das KonTraG eine Unternehmensvorsorge und ein Risiko-Management, wozu thematisch auch die IT-Sicherheit zählt. Für Unternehmen, die an amerikanischen Börsen notiert sind, gilt der Sarbanes Oxley Act (kurz. SOX), der sich mit Risiken von Finanzdaten befasst.

Die so genannten nationalen Krypto-Regulierungen können in Staaten, die solche erlassen haben, den Einsatz bestimmter Verschlüsselungsverfahren durch ein Unternehmen an Bedingungen knüpfen. In Deutschland sind solche Regelungen für die Nutzung von Kryptoverfahren nicht erlassen worden. Dies kann jedoch in anderen Staaten abweichend gehandhabt werden: Meist geht es darum, dass der Einsatz besonders sicherer Verfahren unter einem staatlichen Genehmigungsvorbehalt steht und ggf. erst nach Schlüsselhinterlegung bei staatlichen Stellen erlaubt ist. Es kann außerdem der Fall eintreten, dass die Einfuhr von Kryptogeräten – auch etwa als Bestandteil eines Laptops oder Notebooks – in ein Land anzumelden ist oder grundsätzlich nicht erlaubt ist.

Bei den gesetzlichen Bestimmungen kann es höchst kompliziert werden, wenn es um ein Unternehmen geht, das Standorte in vielen Ländern aufweist. In jedem Land ist dann den dort geltenden gesetzlichen Vorgaben zu genügen. Möglicherweise ist es unpraktisch, alle diese Vorgaben in der Sicherheitsleitlinie aufzuführen. Hier bietet sich an, je Standort ein separates Dokument anzulegen und auf diese Dokumente in der Sicherheitsleitlinie nur zu verweisen.

– Verträge mit Kunden bzw. Bedingungen in Ausschreibungen können Auswirkungen auf die Sicherheit und die Sicherheitsmaßnahmen haben.

Gegenstand von solchen Verträgen können Anforderungen an die Verfügbarkeit von Dienstleistungen bzw. Geschäftsprozessen sein. In Ausschreibungen kann es beispielsweise um die Vertraulichkeitseinstufung der zu verarbeitenden Daten oder um Service-Levels und Reaktionszeiten gehen. Solche Vorgaben können Auswirkungen auf das Sicherheitskonzept haben.

– Eine dritte Quelle für Maßnahmen können unternehmenseigene Regeln sein.

Bereits bestehende Vorgaben etwa zur Anwendung bestimmter Verschlüsselungsverfahren oder zum Einsatz bestimmter Virenschutz-Produkte sind ein wichtiger Input für das Sicherheitskonzept. Solche Vorgaben findet man vor allem in der Sicherheitsleitlinie von Konzernen, um Interoperabilität und Einheitlichkeit zu erreichen. Häufig findet man auch Regeln zur Einstufung und Klassifizierung von Informationen, Daten und Systemen (s. Kapitel 4).

5. Organisationsbeschluss

Aus den vorhergehenden Gliederungspunkten ergibt sich die Konsequenz, ein Sicherheitsmanagement einzurichten und diesem gewisse Kompetenzen, Ressourcen sowie Pflichten zu übertragen. In manchen Sicherheitsleitlinien findet man dazu entsprechende Aussagen – dies kann jedoch auch mit anderen internen Unterlagen erfolgen.

6. Verpflichtungserklärung

Im Grunde ist jeder Mitarbeiter einer Institution gehalten, die Sicherheitsgrundsätze zu kennen und an seinem Arbeitsplatz einzuhalten. Die Sicherheitsleitlinie gelesen und verstanden zu haben sowie sich zu ihrer Einhaltung zu verpflichten, ist Gegenstand einer Verpflichtungserklärung, die von jedem Mitarbeiter zu unterzeichnen ist. Sie ist im Allgemeinen Bestandteil der Personalakte. Der Text der Verpflichtung kann als letzter Absatz der Sicherheitsleitlinie beigefügt oder aber in einem separaten Dokument aufgeführt sein.

6.2 Management der Sicherheitsleitlinie

Umfang

Es wird immer die Frage gestellt, wie umfangreich eine Sicherheitsleitlinie sein muss: Eine Sicherheitsleitlinie ist immer ein „top level“ Dokument auf einem hohen Abstraktionsniveau. Schaut man sich den Gliederungsvorschlag zu Beginn dieses Kapitels an, so stellt man fest, dass der Umfang vor allem von der Länge der Beschreibung des Anwendungsbereichs und von dem Abstraktionsgrad bei der Beschreibung der Gefährdungen abhängt. Als Faustregel gilt, dass ein Umfang von 10 Seiten nicht überschritten werden sollte. Was man auf 10 Seiten nicht aufschreiben kann, gehört nicht in eine Sicherheitsleitlinie, sondern vermutlich schon eher in ein Sicherheitskonzept.

In Kraft setzen

Die Verantwortung für die IT-Sicherheitsleitlinie liegt bei der Unternehmensleitung. Gleichwohl wird ihre Erstellung meist an den IT-Sicherheitsbeauftragten oder an externe Berater delegiert. Die Sicherheitsleitlinie wird Gegenstand von Abstimmungen im oberen Management sein, bevor sie akzeptiert und in Kraft gesetzt wird. Es empfiehlt sich deshalb festzulegen,

- wer in den Abstimmungsprozess einzubeziehen ist,
- wer die Schlussredaktion übernimmt,
- wie und wann die Gegenzeichnung durch die Unternehmensleitung erfolgen soll.

Für diese Prozesse ist entsprechend Zeit einzuplanen.

Wartung

In der Diskussion des PDCA-Zyklus für die Leitung ist bereits der Aspekt der Wartung der Sicherheitsleitlinie genannt worden. Änderungsbedarf entsteht vor allem dann, wenn der Anwendungsbereich geändert wird, grundsätzlich neue Gefährdungen oder Vorgaben zu betrachten sind. Dennoch gilt das Ziel, die Sicherheitsleitlinie so zu schreiben, dass sie möglichst lange unverändert bleiben kann: Jede Änderung würde automatisch Anpassungen am Sicherheitskonzept und seinen mitgeltenden Dokumenten und damit eventuell sogar Änderungen auf der Maßnahmenseite nach sich ziehen. Bei dem damit verbundenen Aufwand sind auch die erforderlichen Abstimmungs- und Genehmigungsprozesse zu berücksichtigen.

7 Grundsätzliches zu Sicherheitsmaßnahmen

Bereits arg strapaziert wurde der Begriff *Sicherheitsmaßnahme* (synonym: Abwehrmaßnahme, Gegenmaßnahme). Wir tragen nach:

Sicherheitsmaßnahme

Jede Maßnahme, die für ein (Informations-, Daten-, System-, Prozess-) Objekt getroffen wird, um Sicherheitsziele für dieses Objekt zu erreichen oder dazu beizutragen, nennen wir eine *Sicherheitsmaßnahme*.

7.1 Maßnahmenklassen

In den vorausgegangenen Kapiteln haben wir bereits verschiedene Sicherheitsmaßnahmen erwähnt. Wir wollen nun eine Klassifizierung dieser Maßnahmen vornehmen:

– Vertragliche Regelungen zum Thema „Sicherheit"

Solche Regelungen können in Arbeitsverträgen, in Verpflichtungserklärungen, in Outsourcing-Verträgen oder in Verträgen mit Kunden und Lieferanten enthalten sein. Sie sind insofern als Maßnahme anzusehen, als damit Mitarbeiter, Outsourcing-Nehmer, Kunden und Lieferanten Regeln erhalten, deren Einhaltung zur Sicherheit beiträgt.

– Organisatorische Regelungen

Hierzu zählen die Festlegung von Rollen und Verantwortlichkeiten (Rechte und Pflichten), Verhaltensregeln, Arbeitsanweisungen und Verfahrensbeschreibungen, Besucherregelungen, Regelungen über Mitnahme von Daten aus dem Unternehmen, Regeln betreffend die private Nutzung von IT-Systemen des Unternehmens, Verbot der Nutzung privater Software im Unternehmen, Passwortregeln.

– Personelle Maßnahmen

Bei diesen Maßnahmen geht es um die Besetzung der definierten Rollen durch qualifiziertes Personal. Die notwendigen Qualifikationen sollten in einem Rollenprofil festgehalten sein: Sie beinhalten Anforderungen an die Ausbildung, Projekt- und Berufserfahrung. Zur Qualifizierung von Personen leisten Sensibilisierung, Schulung und Training (Awareness-Maßnahmen) einen wichtigen Beitrag.

– Infrastruktur-Maßnahmen

Sie dienen der Absicherung von „Sicherheitszonen“: Hierzu zählen die Sicherung des Zugangs zur Sicherheitszone z. B. durch Überwachungseinrichtungen, alarmgesicherte Türen und Fenster, die geschützte Verlegung von Versorgungsleitungen und Datenkabeln, Maßnahmen gegen Elementarereignisse (z. B. Brandschutz), akustische und elektromagnetische Abschirmung der Räumlichkeiten (Abstrahlschutz bzw. -minderung).

– Technische Sicherheitsmaßnahmen

Sicherheitsfunktion

Für Maßnahmen dieser Klasse, z. T. auch für Infrastrukturmaßnahmen, verwendet man in internationalen Standards den Begriff *Sicherheitsfunktionen*. Die Zugriffskontrolle bei Linux, eine Verschlüsselung von Emails, die sichere Schlüsselspeicherung in einer Kryptobox, die Kamera-Überwachung von Sicherheitszonen, die Abschirmung eines Rechners im Sinne von Abstrahlschutz sind Beispiele für solche Sicherheitsfunktionen. Sicherheitsfunktionen finden sich in Betriebssystemen, in Anwendungssoftware und werden z. T. auch durch Einsatz spezieller Sicherheitssoftware und -hardware realisiert.

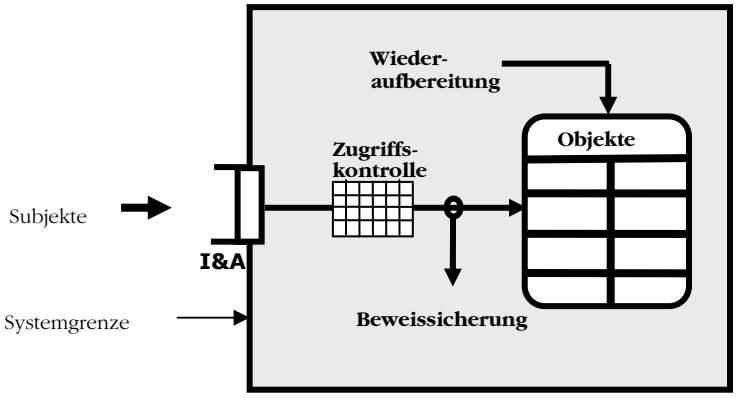

Abbildung 18: Übersicht über C2-Systeme

C2-Klasse

Die Abbildung 18 gibt einen Überblick über die Sicherheitsfunktionen von Betriebssystemen und Datenbanken, die nach der Klasse **C2** aus /TCSEC/ bzw. /CC/ zertifiziert worden sind. Sie besitzen aufeinander abgestimmt eine Identifikation und Authentisierung (I&A) der Benutzer, eine Zugriffskontrolle, eine Beweissicherung sowie eine Wiederaufbereitung gelöschter Objekte. Dieser Standard-Satz von Sicherheitsfunktionen ist heute in vielen kommerziellen Betriebssystemen und Datenbanken enthalten und bildet meist auch das Rückgrat von technischen Sicherheits-

konzepten. Details zu diesen Sicherheitsfunktionen finden Sie im Kapitel „11. Technische Sicherheitsmaßnahmen“.

7.2 Validierung von Maßnahmen

Bei der Erstellung eines Sicherheitskonzeptes geht es im Kern immer darum, den ermittelten Bedrohungen „adäquate“ Sicherheitsmaßnahmen gegenüberzustellen. Dabei trifft man häufig auf die Situation, dass es mehrere Alternativen für entsprechende Maßnahmen gibt.

Validierung

Die richtige Auswahl zu treffen, ist nicht immer einfach: Man sollte sich ein Schema zurechtlegen, nach dem man Sicherheitsmaßnahmen für den vorgesehen Zweck bewertet bzw. *validiert*.

Bei der *Validierung* von Sicherheitsmaßnahmen sollte man mindestens folgende Kategorien berücksichtigen:

1. Eignung

Die geplante Sicherheitsmaßnahme sollte prinzipiell geeignet sein, den betrachteten Bedrohungen zu *begegnen* (Typ 2) bzw. den erwarteten Schaden zu *mindern* (Typ 1). „Prinzipiell geeignet“ meint, dass sich die Sicherheitsmaßnahme gegen die betrachtete Bedrohung richtet oder den Schaden reduziert – ohne schon zu diskutieren, ob dies ausreichend ist. Beispiel: Für den „Schutz der Vertraulichkeit von Daten“ ist z. B. die Protokollierung von Zugriffen keine geeignete Sicherheitsmaßnahme (was sollte sie bewirken?), dagegen ist die Verschlüsselung der Daten prinzipiell geeignet.

2. Wirksamkeit

Die geplante Sicherheitsmaßnahme sollte ausreichend stark sein, um das betrachtete Angriffspotenzial *abzuwehren* (Typ 2) bzw. den erwarteten Schaden *ausreichend* zu mindern (Typ 1). Bleiben wir bei dem Beispiel aus dem Abschnitt zur Eignung: Bei der Wirksamkeit geht es darum, ob wir ein *ausreichend starkes* Verschlüsselungsverfahren auswählen, das dem Angriffspotenzial (Kenntnisse, Zeit, Werkzeuge,…) der betrachteten Angreifer widerstehen kann.

3. Zusammenwirken

Die geplante Sicherheitsmaßnahme soll nicht genutzt werden können, um andere Sicherheitsmaßnahmen zu unterlaufen. Ein Beispiel hierzu: Um die Vertraulichkeit von Daten zu sichern, soll Verschlüsselung eingesetzt werden. Die benötigten Schlüssel werden auf einem nicht am Netz hängenden PC erwürfelt, auf einem Datenträger an die Kommunikationspartner übergeben und sodann in das jeweilige Mailsystem des Nutzers importiert. Anschließend werden die Datenträger vernichtet. Da die Schlüssel auf dem separaten PC gespeichert bleiben, kann bei Verlust

oder Zerstörung des Schlüssels für das Mailsystem des Nutzers schnell Abhilfe geschaffen werden. Da ein Backup-Verfahren im Unternehmen existiert, das die Daten aller Rechner sichert, werden auch die Daten des Schlüssel-PC von Zeit zu Zeit gesichert. Die Backup-Tapes werden ausgelagert, aber ansonsten nicht weiter geschützt. In diesem fiktiven Beispiel unterläuft die Sicherheitsfunktion „Backup aller Daten" die Sicherheit der Verschlüsselung, da die Backup-Tapes nicht gegen den Verlust der Vertraulichkeit geschützt werden. Unbefugte könnten sich Kopien der im Einsatz befindlichen Schlüssel verschaffen.

4. Praktikabilität

Die geplante Sicherheitsmaßnahme soll praktikabel[29], d. h. von den Betroffenen leicht einhaltbar bzw. nutzbar und bei Umsetzung und Anwendung wenig fehleranfällig sein. Komplexe Arbeitsvorgänge besitzen automatisch Fehlerquellen und untergraben damit die Praktikabilität einer Sicherheitsmaßnahme. Umfangreiche oder unverständliche Dokumentation kann zum gleichen Resultat führen. Eine *praktikable* Sicherheitsmaßnahme ist also im Grunde immer eine einfache, leicht erklärbare und befolgbare Maßnahme.

5. Akzeptanz

Die geplante Sicherheitsmaßnahme soll von den jeweils Betroffenen nicht als physisch beeinträchtigend, als unzumutbare Erschwernis oder als sozial diskriminierend angesehen werden. Gegenbeispiele hierfür sind etwa Zugriffskontrollen, die

- auf dem Scannen des Augenhintergrunds durch Laser und Vergleich mit einem gespeicherten Muster (Vermutung der physischen Beeinträchtigung) oder
- auf dem Abnehmen des Fingerabdrucks und Vergleich mit einem gespeicherten Muster (Stigmatisierung als Kriminelle)
- auf dem fehlerfreien Eintippen längerer Erkennungssätze zum Zwecke der Authentisierung (unzumutbare Erschwernis) beruhen.

Bei der Akzeptanz geht es nicht darum, ob eine physische Beeinträchtigung oder eine Diskriminierung *tatsächlich* stattfindet: Wesentlich ist hier die „Psychologie".

6. Wirtschaftlichkeit

Im Zusammenhang mit der Bedrohungsanalyse hatten wir bereits diesen Validierungsfaktor „erkannt": Der Aufwand für die Umsetzung und die Nutzung der geplanten Sicherheitsmaßnahme soll in einem sinnvollen Verhältnis zum reduzierten Risiko stehen.

[29] In Standards gelegentlich „Ease of Use" genannt.

Eine solche Abwägung ist für Bedrohungen vom Typ 1 meist leicht möglich: Der Schaden- bzw. Risikoanalyse können wir entnehmen,

- welche Schadenreduktion x unsere Maßnahme bewirken würde[30],
- welche Kosten y durch diese Maßnahme entstehen[31].

Wirtschaftlichkeit ist immer dann gegeben, wenn $y \leq x$ ist. Sofern bei Bedrohungen vom Typ 2 eine solche Betrachtung nicht durchgeführt werden kann, weil geeignete Zahlen über die Häufigkeiten und Schadenreduktion fehlen, nutzen wir zumindest einen Kostenvergleich, um aus mehreren möglichen Sicherheitsmaßnahmen die „kostengünstigste" herauszufiltern. Unter Umständen kann man fehlendes Zahlenmaterial aus eigener Erfahrung beisteuern, Hinweise von Sicherheitsexperten oder Schwachstellen-Informationsdiensten (CERT-Advisories, CERT = Computer Emergency Response Team) auswerten.

7. Angemessenheit

Die Art der Sicherheitsmaßnahme soll in einem angemessenen, d. h. sinnvollen Verhältnis zur Bedeutung[32] des betroffenen Geschäftsprozesses für seinen Betreiber stehen. Dieser Faktor „Angemessenheit" bietet ein Korrektiv, wenn alle anderen Validierungsfaktoren zwar abgehakt werden konnten, man aber dennoch den Eindruck hat, entweder über das Ziel hinaus zu schießen oder zu „untertreiben".

Bei jeder geplanten Sicherheitsmaßnahme sollten Sie diese sieben Faktoren einzeln diskutieren. Von der Realisierung von Maßnahmen, die in einer oder mehreren dieser Kategorien klare Defizite besitzen, sollten Sie absehen und Alternativ-Maßnahmen untersuchen.

---

30 Ggf. richtet sich die Maßnahme gegen mehrere Bedrohungen, dann summieren wir die Risiken bzw. die Schadenreduktion natürlich über alle entsprechenden Bedrohungen.

31 Bei den Kosten und den Schäden muss man sich auf einen Zeitraum festlegen, für den diese Bilanzierung gelten soll.

32 An dieser Stelle könnte man auch die Begriffsbildung *Schutzbedarf* verwenden.

8 Das Sicherheitskonzept

8.1 Grundsätzliches

Ein Sicherheitskonzept ist immer ein geschriebenes *Dokument*. Diese banale Forderung schließt aus, dass alle sicherheitsrelevanten Details nur in den Köpfen einiger Verantwortlicher vorhanden sind, aber nie schriftlich fixiert werden.

Ähnlich wie bei der Sicherheitsleitlinie gilt auch für das Sicherheitskonzept der Grundsatz „Weniger ist oft mehr", d. h. der Umfang eines Sicherheitskonzeptes ist eher gegenläufig zu seiner Qualität.

Umfang

Die Standardfrage nach dem Umfang eines Sicherheitskonzeptes ist nicht einheitlich zu beantworten: Je nach Unternehmen und Anwendungsbereich sowie dem angestrebten Sicherheitsniveau kann es Sicherheitskonzepte mit 50 Seiten, aber auch mit 500 Seiten geben.

In der Praxis ist vor allem darauf zu achten, eine klare Gliederung einzuhalten, Redundanzen zu vermeiden und nur das zu beschreiben, was zur Umsetzung der Sicherheitsleitlinie nötig ist.

Redundanzen

Redundanzen vermeiden heißt hier insbesondere, nicht den vollständigen Text oder einzelne Passagen

- der Sicherheitsleitlinie oder
- der „sonstigen Vorgaben" wie Gesetzestexte, Vertragstexte und Richtlinien

zu wiederholen. Stattdessen sollten bei Bedarf Verweise auf diese Texte eingefügt werden.

Dokumenten-Hierarchie

Eng mit diesem Punkt hängt auch die Vorgehensweise zusammen, alle Dokumente des Sicherheitsmanagements in einer Pyramide anzuordnen (s. Abschnitt „2.4 Management der Dokumentation"): Jedes Dokument konkretisiert die Ausführungen von Dokumenten, die in der Pyramide eine Stufe höher stehen. Alle Angaben müssen also auf Dokumente der nächsthöheren Stufe abbildbar sein. Dies wird man nicht immer in voller Schönheit hinbekommen, zeigt aber die Zielrichtung auf.

Vollständigkeit

Es ist darauf zu achten, dass ein Sicherheitskonzept vollständig ist, d. h. *alle* konzeptionellen Überlegungen zur Sicherheit sind in genau diesem Dokument enthalten. Es wird dringend davon abgeraten, thematisch zu differenzieren und für jedes Thema ein eigenes Konzept zu erstellen – und dies vielleicht noch durch unterschiedliche Autoren. Dies führt schnell zu Inkonsistenzen und Widersprüchen, z. T. mit fatalen Folgen wie das folgende, gar nicht so fiktive Beispiel zeigt:

In einem Unternehmen werden die Themen „Virenschutz" und „Sicherer Email-Verkehr" in getrennten Dokumenten konzeptionell bearbeitet. Während nun der Autor des Virenschutz-Konzeptes ein Virenschutz-Produkt auf dem entsprechenden Gateway zum Scannen aller ein- und ausgehenden Emails einsetzen möchte, hat der Autor des Email-Konzeptes die Ver- und Entschlüsselung aller mit Partnern auszutauschender Emails am jeweiligen Arbeitsplatz des Absenders bzw. Empfängers vorgesehen. Aufgrund fehlender Kooperation und dafür benötigter Zeit sowie des üblichen Schubladen-Denkens bemerkt niemand, dass die geplanten Maßnahmen zwar isoliert betrachtet nicht zu beanstanden sind, aber in dieser Kombination keinen Sinn machen…

Wird ein solcher fataler Widerspruch nicht oder erst spät entdeckt, kann dies weitreichende Folgen haben. Solche Pannen können sehr kostenträchtig sein.

Listen anlegen

Bevor wir nun in die Ausgestaltung des Sicherheitskonzeptes einsteigen, legen wir folgende Listen bereit, in die wir später Daten eintragen:

- Liste der Objekte
- Liste der Subjekte
- Liste der Bedrohungen
- Liste der bereits vorhandenen Maßnahmen
- Liste der Schwachstellen

Falls Sie beim Blättern den Eindruck gewinnen, dass alles höchst kompliziert ist: Sie haben recht. Deshalb der dringende Rat: Ein *einfaches* Sicherheitskonzept ist immer noch besser als gar kein Sicherheitskonzept. Nehmen Sie deshalb beim ersten „Durchlauf" Vereinfachungen vor, indem Sie Objekte und Subjekte stark gruppieren, Sicherheitsziele mit „ja" und „nein" eintragen (noch ohne Skalierungen), Bedrohungen auf einem summarischen Level (eher im Sinne von Gefährdungen) darstellen. Nach Abschluss dieser ersten Runde werden Sie das Gerüst eines Sicher-

heitskonzeptes haben, das sich in weiteren Runden ausbauen und präzisieren lässt.

8.2 Gliederung des Sicherheitskonzeptes

Als Gliederung für ein Sicherheitskonzept wird der folgende Aufbau vorgeschlagen:

1. Vorspann mit Management Summary, Glossar, Verzeichnisse
2. Gegenstand des Sicherheitskonzeptes
3. Ergebnis der Anforderungsanalyse
4. Objekteigenschaften
5. Subjekteigenschaften
6. Bedrohungsanalyse
7. Maßnahmenauswahl
8. Schwachstellenanalyse
9. Validierung der Maßnahmen
10. Restrisiko-Betrachtung

Wir wollen diese Abschnitte eines Sicherheitskonzeptes im Einzelnen behandeln.

Methodenwahl

Die Gliederungspunkte 4 bis 8 (und teilweise auch 10) sind methodenabhängig, d. h. die ausgewählte Methode für Analysen (s. Kapitel 5 „Analysen“) schlägt hier voll durch.

Wir gehen im Folgenden aus von der Methode aus Abschnitt 5.4 „Ein Ansatz auf der Basis der ISO 15408“. Wenn Sie eher an der der Vorgehensweise nach ISO 27001 / ISO 13335 interessiert sind, lesen Sie weiter im Abschnitt 8.13 „Sicherheitskonzept“ nach ISO 27001“.

Beim IT-Grundschutz ist eine grundsätzlich andere Vorgehensweise erforderlich, auf die wir nicht weiter eingehen – sie ist in /BSI100-2/ eingehend beschrieben.

Wir verwenden im Folgenden ein einfach gestricktes Beispiel, um die Tabellen und Auswertungen zu erläutern. Aus Platzgründen können wir dieses Beispiel dennoch nicht in allen Einzelheiten behandeln.

8.3 Vorspann

Management Summary

Das Management Summary soll in kurzer und prägnanter Form das Ergebnis des Sicherheitskonzeptes für das Management des Unternehmens zusammenfassen:

- Konnten die Vorgaben der Sicherheitsleitlinie konzeptionell umgesetzt werden?
- Mit welchem Aufwand bzw. zu welchen Kosten ist die Realisierung des Sicherheitskonzeptes zu erreichen?
- Gibt es in Einzelbereichen Probleme etwa der Art, dass bestimmte Anforderungen und Ziele zu hoch gesteckt und deshalb gar nicht oder nur zu exorbitanten Kosten umgesetzt werden können? Gibt es in diesen Fällen Alternativen?
- Welches Restrisiko verbleibt nach Umsetzung aller vorgeschlagenen Maßnahmen und wie soll damit umgegangen werden?

Vom Umfang her sollte sich das Summary auf wenige Seiten – maximal drei – beschränken. Alternativ ist es natürlich auch möglich, das Summary als getrenntes Dokument zu erstellen.

Glossar, Verzeichnisse

Zum Thema „Glossar“ und der hierdurch erreichbaren Klarheit von Begriffen mit der Folge präziserer Konzepte wurde schon im Abschnitt 2.4 einiges gesagt – wir lassen es dabei bewenden.

Der besseren Lesbarkeit des Sicherheitskonzeptes wegen sollten Verzeichnisse der Kapitel, Abbildungen und Quellen nicht fehlen.

8.4 Gegenstand des Sicherheitskonzeptes

In diesem Abschnitt legen wir den Gegenstand des Sicherheitskonzeptes, d. h. seinen Anwendungsbereich fest, beispielsweise auf

- die IT und Netze bestimmter Organisationseinheiten des Unternehmens,
- die gesamte IT des Unternehmens einschließlich des Netzwerks mit seinen Übergängen zum Internet,
- einzelne oder alle IT-Anwendungen,
- einzelne oder alle Geschäftsprozesse des Unternehmens.

Damit das Sicherheitskonzept nicht schon an dieser Stelle vom Umfang her aus dem Ruder läuft, lassen wir alle Detail-Informationen die IT-Systeme, Personal und Rollen, Infrastruktur und

Geschäftsprozesse betreffend aus und verweisen auf die Dokumentation dieser Themen, wie wir sie im Kapitel „3. Grundstrukturen der IT-Sicherheit“ erläutert haben.

Vielfach wird man Sicherheitskonzepte für das *gesamte* Unternehmensnetz oder für *alle* Geschäftsprozesse eines Unternehmens schreiben. Die natürliche Grenze bildet dann in der Technik meist der Übergang zum Internet, dem besondere Aufmerksamkeit zu widmen ist. Bei den Geschäftsprozessen liegt die Grenze in den Schnittstellen zu Prozessen der Kunden oder Lieferanten.

Abgrenzung

Immer dann jedoch, wenn das Sicherheitskonzept *nicht* alle Geschäftsprozesse bzw. *nicht* das gesamte Unternehmensnetz umfassen soll, ist es nötig, den zu betrachtenden Teil von den anderen Teilen abzugrenzen: Wird beispielsweise ein Konzept für die IT einer einzelnen Abteilung geschrieben, ist zu klären,

- wo die Grenze zum umfassenderen Unternehmensnetz ist (am Besten auf dem Netzplan die Abteilungs-IT als „Sicherheitszone“ rot markieren),
- auf welche Sicherheitseigenschaften der Unternehmens-IT man sich verlässt bzw. welche Bedrohungen von dort in die Abteilungs-IT importiert werden könnten,
- welche Bedrohungen ggf. aus der Abteilungs-IT in die Unternehmens-IT exportiert werden.

Es soll an dieser Stelle nicht verschwiegen werden, dass solche Teilkonzepte manchmal schwieriger zu schreiben sind als umfassende Konzepte, weil man eben nicht sauber abgrenzen kann und weil man viele Annahmen über die Umgebung treffen muss, die in Praxis letztlich schwer umzusetzen sind. Hier kann ein Teil-Sicherheitskonzept schnell zur Farce werden.

8.5 Ergebnis der Anforderungsanalyse

Ziel und Zweck der Anforderungsanalyse haben wir in Abschnitt 5.4 behandelt. An dieser Stelle des Sicherheitskonzeptes legen wir eine Tabelle an, in die wir Zeile für Zeile

- die jeweilige Vorgabe aus Gesetzen und Verordnungen, Verträgen, sonstigen Regeln und daneben
- die Schlussfolgerungen wie zusätzliche Bedrohungen, weitere Sicherheitsziele, geforderte Maßnahmen, sonstige Informationen wie z. B. über das unterstellte Angriffspotenzial

eintragen. Auf diese Weise wird die Anforderungsanalyse nachvollziehbar dokumentiert. Soweit sich hier neue Bedrohungen oder sogar konkrete Maßnahmen ergeben haben, tragen wir diese in die Liste der Bedrohungen bzw. Maßnahmen ein. Wenn Sicherheitsziele für bestimmte (Informations-, Daten-, System- und Prozess-) Objekte genannt werden, tragen wir die entsprechenden Objekte mit diesen Zielen in die Objekttabelle ein.

8.6 Objekteigenschaften

Im Kapitel „3. Grundstrukturen der IT-Sicherheit“ haben wir bereits Informations- und Datenobjekte, System- und Prozess-Objekte kennen gelernt. Wir betrachten nunmehr ausschließlich zu *schützende* Objekte dieser Art, d. h. solche, für die Sicherheitsziele vorgegeben sind, denen reale Bedrohungen gegenüberstehen. Bei der Vielzahl von Objekten – man denke nur an die meist unüberschaubare Anzahl von Dateien – macht es keinen Sinn, für jedes einzelne Objekt die erforderlichen Analysen durchzuführen. Vielmehr bedienen wir uns des Tricks der „Gruppierung von Objekten“ (s. Kapitel „4. Sicherheitsziele auf allen Ebenen“). Im Folgenden meint „Objekt“ also immer eine geeignete Gruppierung von Einzelobjekten. Für jedes Objekt dieser Art benötigen wir eine Reihe von Informationen (Tabelle 11):

Tabelle 11: Objektinformationen

Objekttyp	Informationen
Informationen/Daten	(alle) Speicher-/Ablageorte (auch temporär, auch beim Transport)
	Vorgegebene Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Missbrauchschutz) und jeweils Höhe der Anforderungen
Technische Systeme	Aufstellungsort (Räume, Leitungsführung)

Objekttyp	Informationen
	Vorgegebene Sicherheitsziele[33] (System-Integrität, System-Verfügbarkeit, System-Missbrauchschutz) und jeweils Höhe der Anforderungen
Geschäftsprozesse	Vorgegebene Sicherheitsziele[34] (Prozess-Integrität, Prozess-Verfügbarkeit, Prozess-Missbrauchsschutz, Verbindlichkeit und Rechtssicherheit) und jeweils Höhe der Anforderungen

Bei den Angaben zu Speicher- und Ablageort bzw. Aufstellungsort verweisen wir – wenn irgend möglich – auf die separate Dokumentation zu unseren Objekten. Mit *Höhe der Anforderungen* ist eine Stufe oder Klasse gemeint, wie wir sie in Kapitel „4. Sicherheitsziele auf allen Ebenen" an Beispielen erläutert haben. Bei der Verfügbarkeit kann dies eine einzelne Prozentangabe oder eine Klasse – z. B. Klasse 1: Verfügbarkeit nicht höher als 90%, Klasse 2: 90-99%, Klasse 3: 99,00-99,75% – sein. Bei der Vertraulichkeit und der Integrität von Informationen und Daten wäre eine Klasse oder eine Einstufung (s. Kapitel 4.1) anzugeben.

Objekttabelle

Mit solchen Informationen füllen wir unsere Objekttabelle. Tabelle 12 gibt die Daten für ein fiktives Beispiel an, das typisch sein könnte für ein KMU im Bereich SW-Entwicklung. Dabei nehmen wir an (s. Kapitel 4), dass für die

- Datenverfügbarkeit die Stufen 1= <95%, 2=95-99%, 3= >99%,
- Datenintegrität die drei Stufen 1 = normal, 2 = mittel, 3 = hoch aus Kapitel 4.1,
- Vertraulichkeit der Informationen die Stufen 1 = offen, 2 = Firmen-vertraulich, 3 = top secret

festgelegt wurden und Missbrauchsschutz als Sicherheitsziel im Beispiel nicht vorkommt. In der Objekttabelle sind nur *Datenobjekte* eingetragen worden. Bei einer ganzheitlichen Analyse würde man einerseits in der Spalte „Vorkommen" auch berück-

33 zusätzlich zu den Zielen für die Datenobjekte

34 zusätzlich zu den Zielen für die Daten- und Systemobjekte

sichtigen, dass diese Informationen in den Köpfen der Mitarbeiter vorkommen, andererseits auch System- und Prozessobjekte hinzufügen, soweit hierfür Sicherheitsziele bestehen. Letzteres dürfte insbesondere bei der Entwicklungsabteilung der Fall sein, in der termingebundene Projekte eine gewisse Verfügbarkeit der Systeme zur Folge haben wird.

Tabelle 12: Objekttabelle (Beispiel)

Objekt	Beschreibung	Vorkommen	Sicherheitsziele	Höhe der Anforderung
O1	Daten der Personal-abteilung	PC der Personalab-teilung, Backup-Tape, Personalakten		
			Vertraulichkeit	3
			Integrität	2
			Verfügbarkeit	1
O2	Daten des Vertriebs	2 PC im Ver-trieb, Backup-Tape, Kunden-Akten		
			Vertraulichkeit	2
			Integrität	3
			Verfügbarkeit	3
O3	Daten der Entwicklungs-abteilung	PC der Ent-wickler, LAN, Backup-Tape, Projektakten		
			Vertraulichkeit	3
			Integrität	2
			Verfügbarkeit	3

Bei Personaldaten ist aufgrund der gesetzlichen Anforderungen im BDSG für die Vertraulichkeit die höchste Stufe vorgesehen worden.

Wichtig ist, diese Tabelle in einer Form zu dokumentieren, die leicht änderbar bzw. wartbar ist. Eine Excel-Tabelle kann dies schon leisten – teuere Werkzeuge zur Inventarisierung sind nicht erforderlich.

8.7 Subjekteigenschaften

Bei der Gefährdungsanalyse (s. Abschnitt 5.4) haben wir

- die Täter(gruppen), die wir als potenzielle Angreifer betrachten,
- andere potenzielle Auslöser und Ursachen von Schäden

ermittelt. Es kommen je nach Kontext in Frage: Innentäter, Unbefugte, Hacker, Wartungspersonal, Reinigungspersonal, Besucher, Befugte, Spione. Bei den anderen Auslösern bzw. Ursachen wären der technische Defekt, Feuer, Blitzeinschlag, Stromausfall als Beispiele zu nennen.

Wir legen nun eine Tabelle mit diesen „Subjekten“ an und stellen einige ihrer Eigenschaften zusammen. Diese Tabelle korrespondiert vom Inhalt her mit der Objekttabelle in Abschnitt 8.6, d. h. wir legen ein vergleichbares Beispiel zugrunde.

Tabelle 13: Subjekttabelle (Beispiel)

Subjekt	Beschreibung	Angriffspotenzial	Schadenpotenzial
S1	Eigene Mitarbeiter	hoch	—
S2	Reinigungspersonal	mittel	—
S3	Externe	hoch	—
S4	Defekte und Ausfälle	—	mittel
S5	Feuer	—	hoch

In der ersten Spalte stehen die Subjekte mit einem Kürzel, in der 2. Spalte tragen wir eine kurze Beschreibung ein. Bei Subjekten, die Personen(gruppen) darstellen, tragen wir in der 3. Spalte deren Angriffspotenzial ein. Bei anderen Auslösern (hier: Defekte, Ausfälle und Feuer) gehen wir analog vor, tragen aber stattdessen in der 4. Spalte das Schadenpotenzial ein. Erläuterungen zu Angriffspotenzial und Schadenpotenzial finden Sie im Abschnitt 5.4 unter „Bedrohungsanalyse“.

8.8 Bedrohungsanalyse

Wir erörtern das Verfahren der Bedrohungsanalyse beispielhaft anhand der Objekt- und Subjekttabellen der beiden vorausge-

gangenen Abschnitte. Alle sich ergebenden Bedrohungen tragen wir in die *Liste der Bedrohungen* ein.

Die Bedrohungsanalyse ist in Form eines *Programms* notiert, woraus man entnehmen kann, dass diese Ableitungen auch maschinell ausgeführt werden können – genau dies tun einschlägige Risikoanalyse-Werkzeuge. In die spitzen Klammern <…> tragen wir jeweils die ausgewählten Werte ein. Aus den beiden Tabellen können wir die Bedrohungen damit wie folgt ableiten:

1. Wir nehmen uns unsere Objekttabelle vor und wählen das erste / nächste *Objekt* <Objekt> aus.
   Falls schon alle Objekte bearbeitet worden sind, ist unser „Programm" beendet.
2. Wir wählen aus der Objekttabelle das erste / nächste Sicherheitsziel <Sicherheitsziel> für unser Objekt aus.
   Falls für das betrachtete Objekt bereits alle Sicherheitsziele abgearbeitet worden sind, gehe zu Schritt 1.
3. Wir wählen aus unserer Subjekttabelle das erste / nächste Subjekt <Subjekt> aus.
   Falls für das betrachtete Objekt und das gewählte Sicherheitsziel bereits alle Subjekte abgearbeitet worden sind, gehe weiter zu Schritt 2.

Damit das Subjekt dem Objekt Schaden zufügen oder es angreifen kann, muss es logischen Zugriff auf oder physischen Zugang[35] zu diesem Objekt haben.

4. Wir wählen für das betrachtete Objekt aus der Objekttabelle das erste / nächste Vorkommen <Vorkommen> aus.
   Falls für das betrachtete Objekt, das gewählte Sicherheitsziel und das betrachtete Subjekt bereits alle Vorkommen abgearbeitet worden sind, gehe zu Schritt 3.
5. Wir prüfen, ob mit den aktuellen Werten <Objekt>, <Sicherheitsziel>, <Vorkommen> das Subjekt als Angreifer bzw. als Auslöser eines Schadens in Frage kommt.
   Dies erkennen wir in der Subjekttabelle an den Eintragungen entweder zum Angriffspotenzial in Verbindung mit der

---

35 Die „Programmlogik" verlangt etwas Abstraktion: *Feuer* hat Zugang zu unseren Objekten, wenn es an dem Ort ausbrechen kann, an dem sich unsere Daten befinden. Ein *Defekt* hat Zugang zu unseren Objekten, wenn er das System betrifft, auf dem unsere Daten gespeichert sind.

Plausibilitätsbetrachtung (s. Abschnitt 5.4) für diesen Angriff oder an den Eintragungen zum Schadenpotenzial. Kommt dieses Subjekt *nicht* als Angreifer bzw. Auslöser in Frage, dann gehen wir zurück zu Schritt 4.

Nun ist ein Angriff plausibel oder ein Schaden tatsächlich in Betracht zu ziehen.

6. Wir tragen folgenden Satz (mit den ausgefüllten Daten in den spitzen Klammern <…>) in unsere Bedrohungsliste ein:

   Bei Bedrohungen vom Typ 1:

   "Das <Subjekt> verletzt das <Sicherheitsziel> für das <Objekt>, indem es für das <Objekt> auf <Vorkommen> ein Schadenpotenzial <Schadenpotenzial> verursacht."

   Bei Bedrohungen vom Typ 2:

   "Das <Subjekt> verletzt das <Sicherheitsziel> für das <Objekt>, indem es das Objekt <Objekt> auf <Vorkommen> mit dem Angriffspotenzial <Angriffspotenzial> angreift."

Spielen wir auf diese Weise der Reihe nach alle Objekte, Sicherheitsziele, Subjekte und Vorkommen durch, erhalten wir eine umfangreiche Liste von realen Bedrohungen. Die Liste in der Tabelle 14 ist der Länge wegen gekürzt: Sie enthält nur die Bedrohungen, die sich auf das Objekt <Personaldaten> und das Sicherheitsziel <Vertraulichkeit> beziehen, soweit dieses durch die Subjekte <Externe> oder <Reinigungspersonal> bedroht ist. Zusätzlich haben wir unterstellt, dass ein Angriff auf die Personaldaten durch <eigene Mitarbeiter> nicht plausibel ist.

Tabelle 14: Liste der Bedrohungen (Beispiel)

Bedrohung	Beschreibung
B1	Externe verletzen die Vertraulichkeit von Personaldaten, indem sie diese Daten auf dem PC der Personalabteilung mit einem Angriffspotenzial "hoch" angreifen.
B2	Externe verletzen die Vertraulichkeit von Personaldaten, indem sie diese Daten auf dem Backup-Tape mit einem Angriffspotenzial "hoch" angreift.
B3	Externe verletzen die Vertraulichkeit von Personaldaten, indem sie diese Daten in den Personalakten mit einem Angriffspotenzial "hoch" angreifen.

Bedrohung	Beschreibung
B4	Reinigungspersonal verletzt die Vertraulichkeit von Personaldaten, indem es diese Daten auf dem PC der Personalabteilung mit einem Angriffspotenzial "mittel" angreift.
B5	Reinigungspersonal verletzt die Vertraulichkeit von Personaldaten, indem es diese Daten auf dem Backup-Tape mit einem Angriffspotenzial "mittel" angreift.
B6	Reinigungspersonal verletzt die Vertraulichkeit von Personaldaten, indem es diese Daten in den Personalakten mit einem Angriffspotenzial "mittel" angreift.

8.9 Maßnahmenauswahl

Maßnahmen haben den Zweck,

- Anforderungen aus einzuhaltenden Gesetzen und Verträgen sowie internen Regeln des Unternehmens (s. Abschnitt 6.1) zu erfüllen,
- die ermittelten Bedrohungen (s. Liste der Bedrohungen im vorherigen Abschnitt) abzuwehren oder zumindest den Schaden zu reduzieren.

Wo erhält man Informationen über mögliche Sicherheitsmaßnahmen?

- Die nachfolgenden Kapitel zur rechtlichen, personellen, infrastrukturellen und technischen Sicherheit enthalten viele Hinweise zu möglichen Maßnahmen.
- Weiterhin findet man in /ISO17799/ eine Reihe von Hinweisen und Beispielen.
- Das Grundschutzhandbuch ist eine umfassende Quelle für Sicherheitsmaßnahmen.
- Sofern Gesetze, Verträge oder unternehmensinterne Vorgaben Maßnahmen vorschreiben, sind diese zu übernehmen.
- Dann bleiben immer noch die Fachliteratur und die Beratung durch Sicherheitsexperten.

Im vorletzten Anstrich kann es sich auch um Vorgaben handeln, die wir bei den Sicherheitszielen (s. Kapitel 4) erläutert haben: Festlegungen, wie Sicherheitsziele zu skalieren und welche Vorgaben bzw. Maßnahmen daran zu knüpfen sind. Diese Vorgaben haben wir in der Objekttabelle in der Spalte *Höhe der Anforderungen* in Form einer Ziffer eingetragen.

Um die Zahl der Maßnahmen zu begrenzen, ist es sinnvoll, Maßnahmen zu wählen, die mehrere bzw. viele Bedrohungen aus unserer Liste *gleichzeitig* abdecken. Wir tragen jede ausgewählte Maßnahme in die Liste der Maßnahmen ein und vermerken, gegen welche Bedrohung sie gerichtet ist bzw. welche Anforderungen aus Gesetzen etc. sie erfüllt. Es kann Bedrohungen geben, die durch keine Maßnahmen abgefangen werden können. Das bedeutet, dass die Maßnahmenspalte an dieser Stelle leer bleibt. Solche Bedrohungen gehen voll in das Restrisiko ein. In der Tabelle 15 zeigen wir einen Ausschnitt einer möglichen Maßnahmenliste zu unserem Beispiel. Die Tabelle beinhaltet noch keine *Validierung* der Maßnahmen. Diese werden wir noch nachtragen.

Tabelle 15: Maßnahmenliste (Beispiel)

Maßnahme	Beschreibung	wirkt gegen
M1	Personaldaten werden auf dem PC der Personalabteilung verschlüsselt gespeichert.	B1, B4
M2	Das Backup-Tape wird in einem Tresor aufbewahrt, zu dem nur der Backup-Manager einen Schlüssel hat.	B2, B5
M3	Personalakten sind bei Abwesenheit des Sachbearbeiters der Personalabteilung und außerhalb der Bürozeiten grundsätzlich im abgeschlossenen Aktenschrank untergebracht. Schlüssel zu diesem Schrank haben der Sachbearbeiter und der Leiter.	B3, B6
M4	Der PC des Sachbearbeiters der Personalabteilung ist bei kurzzeitiger Abwesenheit zu sperren (Bildschirm-Sperre, Passwort).	B1, B4
M5	Der Büroraum der Personalabteilung ist bei Abwesenheit des Sachbearbeiters zu verschließen. Außer dem Sachbearbeiter haben nur der Leiter und das Reinigungspersonal einen Schlüssel zu diesem Raum.	B1, B3, B4, B6

8.10 Schwachstellenanalyse

Die Liste der Bedrohungen verlängert sich, sobald man für die betrachteten Systeme und die ausgewählten Sicherheitsmaßnahmen mögliche Schwachstellen ermittelt und analysiert. Das Schema der Auswertung von Schwachstellen ist in Abschnitt 5.5 dargestellt worden. Jede nach der Auswertung übrig bleibende Schwachstelle ist eine weitere Bedrohung, die in unsere Liste eingetragen werden muss.

Wenn es Maßnahmen gibt, um eine Schwachstelle zu beheben oder teilweise zu kompensieren, trägt man diese analog in die Maßnahmenliste ein und gibt an, gegen welche Bedrohung – hier also die sich aus der Schwachstelle ergebende – sie wirkt. Gibt es solche Maßnahmen nicht, schlägt die betreffende Schwachstelle beim Restrisiko voll durch.

In unserem Beispiel wollen wir fiktiv annehmen, dass der PC der Personalabteilung ein Betriebssystem mit einer bekannten Schwachstelle besitzt, nämlich über ein „geheimes“ Passwort für die Wartung des Systems jederzeit Zugang zum PC zu bekommen, wodurch man ein Programm installieren kann, das die Verschlüsselung umgeht, d. h. aus Sicht der Sicherheit hat die Sicherheitsmaßnahme „Verschlüsselung“ eine Schwachstelle – man kann sie umgehen. Diese Schwachstelle bewerten wir wie in Abschnitt 5.5 beschrieben. Wir nehmen an, dass es sich um eine *ausnutzbare* Schwachstelle handelt. Sie beeinträchtigt das Sicherheitsziel Vertraulichkeit. Wir unterstellen, dass ein Angriffspotenzial der Stufe „mittel“ zur Durchführung des Angriffs ausreicht. Aus der Subjekttabelle entnehmen wir, dass dies auf die Subjekte „Reinigungspersonal“ und „Externe“ zutrifft. Die Frage, ob ein solcher Angriff plausibel ist, sei mit „ja“ beantwortet. Folglich müssen wir unsere Bedrohungsliste um die Schwachstelle X erweitern (Tabelle 16):

Tabelle 16: Bedrohungen aus Schwachstellen

B7	Externe verletzen die Vertraulichkeit von Personaldaten, indem sie diese Daten durch Ausnutzen der Schwachstelle X angreifen.
B8	Reinigungspersonal verletzt die Vertraulichkeit von Personaldaten, indem es diese Daten durch Ausnutzen der Schwachstelle X angreift.

Man kann nun einwenden, dass das Abschließen des Raums (Maßnahme M6) das Ausnutzen der Schwachstelle durch Externe ausschließt. Beim Reinigungspersonal wäre das aber zu vernei-

nen, da dieses einen Schlüssel zum Raum besitzt und üblicherweise unbeaufsichtigt, außerhalb der Bürozeiten tätig wird. Damit wäre ggf. B7 durch die Maßnahme M6 kompensiert, keinesfalls aber B8.

8.11 Validierung der Maßnahmen

Unsere Maßnahmentabelle verlängern wir durch je eine Spalte für jeden ausgewählten Validierungsfaktor (s. Abschnitt 7.2) und tragen dort jeweils das Ergebnis der Validierung ein. Den Faktor „Wirksamkeit“ wollen wir an unserem *Beispiel* noch etwas näher beleuchten: Die Beurteilung, ob unsere Maßnahmen (s. Maßnahmentabelle für das Beispiel) gegen die angegebenen Bedrohungen ausreichend wirksam sind, verlangt die Ermittlung der Mechanismenstärke dieser Maßnahmen. Ist diese „hoch“, wäre insofern alles klar, als damit sowohl die Externen als auch das Reinigungspersonal geblockt würden. Ist sie jedoch nur „mittel“, hätten wir mit dem Angreifer „Externe“ ein Problem…

Sofern sich eine Maßnahme als unwirksam herausstellt, muss man natürlich die anderen Faktoren nicht mehr auswerten.

Bei der Akzeptanz der Maßnahme M5 (Abschließen des Raumes) haben wir „fraglich“ eingetragen (Abbildung 19), weil nicht zu erwarten ist, dass dies auch bei jeder kurzfristigen Abwesenheit tatsächlich geschieht.

Maßnahme	...	wirkt gegen	Eignung	Wirksamkeit	Zusammenwirken	Praktikabilität	Akzeptanz	Wirtschaftlichkeit	Angemessenheit
M1	...	B1, B4	ja	Schwachstelle					
M2	...	B2, B5	ja	ja	ok	ja	ja	ja	ja
M3	...	B3, B6	ja	ja	ok	ja	ja	ja	ja
M4	...	B1, B4	ja	ja	ok	ja	ja	ja	ja
M5	...	B1, B3, B4, B6	ja	ja	ok	ja	fraglich	ja	ja

Abbildung 19: Validierungstabelle (Beispiel)

Im Ergebnis ist festzustellen, dass

- M1 eine Schwachstelle besitzt und insofern unwirksam ist – hier muss nachgebessert werden,
- M5 ein Akzeptanzproblem besitzt, das man ggf. durch Wahl einer anderen Maßnahme ausräumen oder aber durch verstärkte Awareness-Maßnahmen kompensieren kann.

8.12 Restrisiko und seine Behandlung

Schlussendlich benötigen wir eine Aussage zum Restrisiko. Wie das Restrisiko bei den einzelnen Bedrohungen (Typ 1 und Typ 2) nach Ergreifen von Gegenmaßnahmen bestimmt wird, haben wir in Abschnitt 5.4 kennen gelernt. Zum Umgang mit dem Restrisiko haben wir in Abschnitt 5.6 Alternativen vorgeschlagen.

Das Restrisiko und der jeweilig vorgesehene Umgang mit ihm tragen wir in weitere Spalten unserer Liste der Bedrohungen ein. Eine abschließende Betrachtung muss durch Auswertung dieser Spalten festhalten, dass alle Restrisiken geeignet behandelt wurden.

8.13 „Sicherheitskonzept" nach ISO 27001

Die Erstellung des Sicherheitskonzeptes erfolgte in den vorausgegangenen Abschnitten nach dem Modell aus 5.4 „Ein Ansatz auf der Basis der ISO 15408". Möchte man nach dem Modell der ISO 27001 vorgehen, muss man sich zunächst mit der spezifischen Begriffswelt und der „etwas anderen" Denkweise beschäftigen[36].

Wir schauen uns zunächst die Struktur der Dokumentation an, die in einem typischen Sicherheitsprozess nach ISO 27001 entsteht:

1 Sicherheitsleitlinie (bestehend aus der ISMS-Leitlinie und der Informationssicherheitsleitlinie),

2 Definition des Anwendungsbereichs[37],

3 Register der Informationswerte,

4 Risikoanalyse und -bewertung,

5 Erklärung zur Anwendbarkeit[38],

6 Behandlung des Restrisikos.

Sicherheitsleitlinie

Typisch ist eine Aufteilung der Sicherheitsleitlinie in zwei Bestandteile: Die *ISMS-Leitlinie* beschreibt alle Vorgaben für die folgenden Schritte, also die Methodenauswahl bei der Risiko-

---

36 Dies wollen wir hier nicht weiter vertiefen, sondern auf weiterführende Literatur verweisen, z. B. auf das Buch /KRS2008/.

37 Im Englischen: Scope.

38 Im Englischen: Statement of Applicability, abgekürzt: SoA.

analyse und -bewertung, Vorgaben zur Akzeptanz von Restrisiken („Akzeptanzschwellen“), die Organisationsform und die Zuständigkeiten für die Informationssicherheit. Die *Informationssicherheitsleitlinie* enthält dagegen die Informationen, die wir im Kapitel 6 „Die Sicherheitsleitlinie“ aufgeführt haben und die gewünschte Sicherheit für das Unternehmen charakterisieren.

Die Dokumente 2 bis 6 stellen genau die Informationen dar, die wir in einem Sicherheitskonzept erwarten. *Ein* Unterschied zur klassischen Vorgehensweise besteht also darin, dass es kein „Sicherheitskonzept“ als eigenes Dokument gibt. Vielmehr sind die wesentlichen Informationen auf mehrere Dokumente aufgeteilt.

Anwendungsbereich

In dieser „Abteilung“ wird festgelegt, worauf sich alles Weitere beziehen soll: Handelt es sich um ein klassisches Vorgehen mit der Betrachtung der (gesamten oder eines Teils der) IT eines Unternehmens oder ist das Modell der Geschäftsprozesse (vielleicht nur eine Auswahl derselben) Gegenstand der Überlegungen. Man kann hier den Kreis groß oder klein ziehen – die Festlegung des Anwendungsbereichs liegt einzig und allein in der Verantwortung des Unternehmens.

Informationswerte

Das Register der Informationswerte[39] beinhaltet die zu schützenden Objekte / Subjekte. Sie sind Gegenstand der nachfolgenden Analysen.

Risiken

Die Identifizierung und Abschätzung (bzw. Klassifizierung) von Risiken haben wir in Kapitel 5 „Analysen“ erläutert – ebenso die Notwendigkeit von Risikobewertungen.

Anwendbarkeit

Bei dem Begriff *Anwendbarkeit* fragt man sich, was soll angewendet werden? Es geht im Grunde um den Anhang A des Standards, in dem so genannte „Maßnahmenziele“ und „Maßnahmen“ aufgeführt[40] sind.

Der umfangreiche Anhang A ist zunächst nach 11 Sicherheitsthemen (wie z. B. Sicherheitsleitlinie, Organisation der Informationssicherheit, Personalsicherheit, Physische und umgebungsbezogene Sicherheit, Sicherstellung des Geschäftsbetriebs) gegliedert. Bei jedem Thema gibt es eine Unterteilung in Kategorien,

---

39 Im Englischen: (Information) Assets.

40 Im Englischen: Control Objectives (= Maßnahmenziele) und Controls (= Maßnahmen).

die sich jeweils mit einem bestimmten Sicherheitsaspekt beschäftigen.

Als Beispiel wählen wir das Thema[41] „Umgang mit Informationssicherheitsvorfällen“ aus und betrachten die beiden im Anhang A vorkommenden Kategorien

A.13.1 Melden von Informationssicherheitsereignissen und Schwachstellen,

A.13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen.

In jeder Kategorie gibt es charakteristisches „Maßnahmenziel“. Für A.13.1 lautet dieses:

„Sicherstellen, dass Informationssicherheitsereignisse und Schwachstellen in Verbindung mit Informationssystemen so kommuniziert werden, dass rechtzeitig korrigierende Aktionen ergriffen werden können.“

Dieses nachvollziehbare Ziel mündet in folgende „Maßnahmen“:

A.13.1.1 Melden von Informationssicherheitsereignissen

„Informationssicherheitsereignisse müssen so schnell wie möglich über die geeigneten Managementkanäle gemeldet werden.“

A.13.1.2 Melden von Sicherheitsschwachstellen

„Alle Angestellten, Auftragnehmer und Drittbenutzer von Informationssystemen und Dienstleistungen müssen verpflichtet sein, alle beobachteten oder vermuteten Sicherheitsschwachstellen in Systemen oder Dienstleistungen festzuhalten und zu melden.“

Man erkennt, dass der Begriff „Maßnahme“ für diese Texte nicht zutrifft. Es handelt sich vielmehr um Sicherheitsanforderungen, die erst in einem weiteren Schritt in konkrete Einzelmaßnahmen münden. Die konkrete Ausgestaltung dieser Einzelmaßnahmen obliegt dem Unternehmen.

In /ISO 17799/ findet man zu diesen „Maßnahmen“ weitere Hinweise, die bei der Auswahl und Beurteilung konkreter Einzelmaßnahmen helfen können. Hierbei ist auch der Maßnahmenkatalog /BSI-M/ des IT-Grundschutzes eine unverzichtbare Quelle.

---

[41] Im Anhang A des Standards trägt dies Thema die Nummerierung A.13. Die folgenden Passagen sind z. T. Zitate aus dem deutschen Normenentwurf.

Nun zurück zu der „*Erklärung der Anwendbarkeit*“: In diesem Dokument ist für jede „Maßnahme“ des Anhangs A zu beurteilen, ob sie für das Unternehmen anwendbar, d. h. zur Erreichung der Sicherheitsziele anwendbar und geeignet ist, oder ob auf diese Maßnahme (begründet) verzichtet werden kann.

Praxistipp

Aus dem Anhang A erstellen Sie eine Liste aller „Maßnahmen“ (als Tabellenspalte) und darüber als Tabellenzeile die Liste der zu schützenden Informationswerte. In der Tabelle tragen Sie anschließend

- ein „Nein“ ein, wenn diese „Maßnahme“ für den betreffenden Informationswert *nicht* umgesetzt werden soll,
- ein „Ja“ ein, wenn die „Maßnahme“ für den betreffenden Informationswert umgesetzt werden soll.

Bei „Nein“ tragen Sie die Begründung ein oder verweisen auf ein Dokument, in dem die Begründung steht. Als Begründung kommen z. B. in Frage:

- Diese „Maßnahme“ ist auf den konkreten Informationswert generell nicht anwendbar.
- Diese „Maßnahme“ leistet keinen Beitrag zu den Sicherheitszielen für diesen Informationswert.
- Diese „Maßnahme“ ist im Vergleich zwischen Risikominderung und Kosten nicht angemessen.

Bei „Ja“ tragen Sie die konkreten Einzelmaßnahmen ein, die Sie zur Erfüllung dieser „Maßnahme“ für den betreffenden Informationswert vorsehen oder bereits getroffen haben. Aus Platzgründen wird man dazu auf ein separates Dokument (nummerierte Maßnahmenliste) verweisen.

Behandlung des Restrisikos

Anhand der erstellten Tabelle ist in jedem Einzelfall zu prüfen, wie sich das Risiko nach Einführung der konkreten Einzelmaßnahmen verändert. Arbeitet man mit Risikoklassen, so sollte erkennbar sein, wie sich die Risikoklasse für jedes Einzelrisiko ändert (in der Regel reduziert).

Im letzten Schritt ist festzulegen, wie man mit diesen Restrisiken weiter verfährt – dazu finden Sie Ausführungen in Abschnitt 5.6 „Umgang mit dem Restrisiko“.

Wichtig ist: Die so entstehende Gesamtdarstellung ist von der Leitungsebene zu unterzeichnen oder anderweitig formal zu billigen („Erklärung“). Die Unternehmensleitung akzeptiert damit die verbleibenden Restrisiken – mit der logischen Folge, dass die

Mittel zur Erreichung des akzeptierten Restrisikos bereitgestellt werden müssen...

9 Rechtliche Sicherheit

Der Umgang mit Daten, die von allgemeinem Interesse und von Wichtigkeit sind, wird zumeist per Gesetz geregelt. In Deutschland sind das Datenschutzgesetz oder das Telekommunikationsgesetz Beispiele solcher Regelungen. Jede Organisation hat bei dem Umgang mit rechtlich sensiblen Daten für die entsprechende rechtliche Sicherheit, d. h. für die Beachtung der geltenden Gesetze durch ihre Mitarbeiter zu sorgen. Das umfangreiche Thema der Rechtssicherheit können wir hier nur streifen und beschränken uns in den nachfolgenden Kapiteln auf folgende Themen aus der Praxis:

Befolgen von Gesetzen

- Anerkennung von Rechtsvorschriften
- Datenschutzgesetze
- Gesetze zum Schutz geistigen Eigentums
- Copyright und Lizenzrecht für Software
- Verwaltung von Medien und Aufzeichnungen

Vermeidung von Strafverfahren

- Vermeidung von Verleumdung und übler Nachrede
- Verwendung von Copyright-geschützten Inhalten aus dem Internet
- Elektronischer Versand von Copyright-geschütztem Material
- Verwendung von Textpassagen direkt aus Reports, Büchern und Dokumenten

Verschiedenes

- Aufzeichnung von Sicherheitsverstößen
- Reservierung von Namen für Web-Domänen
- Risikoversicherungen
- Aufzeichnung von Telefongesprächen
- Non Disclosure Agreements

9.1 Befolgen von Gesetzen

Anerkennung von Rechtsvorschriften

Bevor wir zu den Details bei den für uns relevanten Gesetzen kommen: Wir müssen durch entsprechende Zusätze in den Arbeitsverträgen grundsätzlich dafür Sorge tragen, dass die Mitarbeiter sich beim Umgang mit sensiblen Informationen ihrer Verantwortung bewusst sind. Diese Verantwortlichkeiten sind ausführlich, explizit und verständlich in den Arbeitsverträgen aufzuführen. Auch ist eine Kontaktadresse für Rückfragen zu rechtlichen Problemen anzugeben. Bei den Mitarbeitern darf nicht das Gefühl entstehen, dass sie bei komplexen, für sie zunächst nicht verständlichen, aber justitiablen Vorgängen alleine gelassen werden. Die Zusätze in den Arbeitsverträgen bezüglich der Einhaltung geltender Gesetze sind für beide Parteien von großer Wichtigkeit, um

- nicht unwissentlich gegen gesetzliche Vorschriften zu verstoßen und
- nicht zu versäumen, ausreichend aufgeklärt und auf die Einhaltung der Gesetze hingewiesen zu haben.

Versäumt das Unternehmen, auf die Einhaltung entsprechender Gesetze in den Arbeitsverträgen hinzuweisen, sind Verstöße und nachfolgende Gerichtsverfahren wahrscheinlich, ohne dass die Verstöße in adäquate disziplinarische Maßnahmen innerhalb des Unternehmens umgesetzt werden können.

Hinweise auf die anzuwendenden gesetzlichen Regelungen, beispielsweise den Umgang mit vertraulichen Daten betreffend, müssen Bestandteil der Sicherheitsleitlinie des Unternehmens sein.

BDSG

Kommen wir nun zum Bundesdatenschutzgesetz (BDSG) – einem der wichtigsten Gesetze zum Schutz von Informationen in Deutschland. Jede Organisation hat das BDSG grundlegend zu beachten. Dieses Gesetz regelt die Bearbeitung, Weitergabe und Speicherung von personenbezogenen Daten in jeder Form. Bei Unkenntnis der Gesetzeslage kann leicht gegen dieses Gesetz verstoßen werden, ohne dass die Verantwortlichen es bemerken. Beispiele dazu sind der Aushang von Geburtstagslisten am schwarzen Brett oder telefonische Auskünfte über Mitarbeiter gegenüber unberechtigten Dritten. Ein weiteres wichtiges Gesetz in Deutschland, welches in diese Rubrik fällt, ist das Telekommunikationsgesetz, das die Vertraulichkeit von Daten bei deren elektronischer Übermittlung regelt.

Aber nicht nur der Umgang mit personenbezogenen Daten unterliegt strengen rechtlichen Vorschriften, auch für Bearbeitung von Daten, die geistiges Eigentum repräsentieren, gibt es entsprechende Gesetze.

Geistiges Eigentum, Copyright

Es gehört zu den Aufgaben des IT-Sicherheitsmanagements, gemeinsam mit der Verwaltung Richtlinien für den Umgang mit Daten, die durch Copyright oder Patente geschützt sind, zu erarbeiten und an die Mitarbeiter zu kommunizieren. Diese Richtlinien regeln insbesondere die Anfertigung von Kopien und Weitergabe von patent- oder Copyright-geschützten Daten. Dies betrifft auch die Erstellung von Dateien und Datenbanken mit geschütztem Material zur internen Verwendung im Unternehmen.

Lizenzen

Wir haben uns in dem vorigen Abschnitt allgemein auf Informationen, die durch strukturierte Daten dargestellt werden, bezogen. Wie sieht es speziell im Falle von Computerprogrammen, also bei der Software aus? Das Kopieren und Verteilen von nicht selbst erstellter Software ist prinzipiell illegal und strafbar – es sei denn, der Verfasser bzw. der Eigentümer der Software hat dies explizit gestattet (OpenSource, Freeware). Die IT-Sicherheitsleitlinie muss in diesem Sinne Vorgaben zum Schutz geistigen Eigentums enthalten. Beim Sicherheitskonzept sind organisatorische Regelungen folgender Art vorzusehen:

- Die Verwendung von Software am Arbeitsplatz ist nur dann gestattet, wenn das Unternehmen eine Lizenz dafür legal erworben hat.
- Software darf im Unternehmen nicht außerhalb des erworbenen Lizenzrahmens kopiert und verteilt werden.
- Kopien von Software dürfen nicht an für das Unternehmen temporär tätige Dritte weitergegeben werden, außer die erworbene Lizenz gestattet dieses explizit.
- Die Lizenzen müssen auf Verlangen (z. B. den Ermittlungsbehörden) vorgelegt werden können.
- Die Einhaltung der Anzahl erlaubter Kopien von Software im Unternehmen ist ständig vom Lizenz-Management zu kontrollieren. Das setzt voraus, dass es innerhalb des Unternehmens eine solche verantwortliche Stelle gibt.
- Vor dem Verkauf gebrauchter Arbeitsplatzrechner an Verwerter sind die Festplatten physikalisch zu löschen. Der Verbleib von Software auf der Festplatte und die damit verbundene Weitergabe an den Verwerter ist ebenfalls ein Verstoß gegen das Lizenzrecht.

– „Shareware“ “ist keine lizenzfreie Software. Bei der Verwendung von Shareware im Unternehmen muss nach der vorgegebenen Evaluationsperiode, meist 30 Tage, die Lizenz erworben oder die Software von allen Rechnern gelöscht werden.

Unberechtigtes Kopieren oder andere Verstöße gegen rechtliche Vorschriften können nicht nur durch Mitarbeiter des *Unternehmens,* sondern auch durch Dritte erfolgen und gehen mit dem eingangs erwähnten Missbrauch von Rechnern, besonders von mobilen Geräten, einher. Deshalb ist dringend anzuraten, Regeln für die ordnungsgemäße Verwendung von Arbeitsplatzrechnern, Notebooks, etc. vorzusehen. Diese Regeln sollten eine Absicherung der Rechner beinhalten, um

– das Kopieren sensibler Daten durch Unbefugte zu verhindern,
– das Manipulieren von sensiblen Daten zu verhindern,
– das Auskundschaften von sensiblen Daten zu verhindern, mit denen weitere Angriffe auf die Infrastruktur des Unternehmens erst ermöglicht werden.

Falls Zugriffe auf die IT-Systeme des Unternehmens nicht explizit unterbunden oder zumindest als nicht autorisiert bezeichnet werden, kann rechtlich eine Duldung oder gar Genehmigung unterstellt werden. Zu beachten sind:

– „Willkommen-Botschaften“, die vor der Anmeldeprozedur auf dem Bildschirm bei dem Zugriff auf ein IT-System erscheinen, können als Aufforderung, Einladung und Erlaubnis interpretiert werden.
– Pre-Login-Informationen, die Leistungsumfang und Merkmale des Systems beschreiben, können unautorisierte Zugriffsversuche (Motto: „Hier gibt es etwas zu holen“) provozieren.

Kommen wir zu dem letzten Punkt dieses Kapitels, der Aufbewahrungspflicht“ von Medien und Aufzeichnungen.

Aufbewahrungspflicht

Häufig verlangt der Gesetzgeber oder eine Zertifizierungsinstanz, die dem Unternehmen ein Gütesiegel verliehen hat, eine „geregelte Archivierung“ von Daten. Dabei steht insbesondere der Schutz der Daten gegen Verfälschung und Verlust im Vordergrund. Ein weiterer wichtiger Aspekt ist die Alterung der Medien und der Aufzeichnungsverfahren – oder besser: der Wiedergabeverfahren. Falls beispielsweise wichtige Daten heute nur noch

auf 8“ SD-Disketten existieren, wird man große Mühen haben, ein passendes Laufwerk und Software zum Auslesen der Daten zu finden. In den Richtlinien für die Archivierung müssen deshalb Regeln zum Umkopieren von Daten auf aktuelle Medien vorhanden sein. Ebenso sind für die Archivierung Richtlinien für die Anwendung kryptografischer Verfahren wie zum Beispiel digitaler Signaturen zu formulieren. Banal ist eine oft vergessene Regelung: Was hat nach Ende der Aufbewahrungsfrist mit den Daten und deren Trägern zu geschehen? Es gibt nur zwei Möglichkeiten:

- Verlängerung der Aufbewahrungsfrist oder
- sichere Vernichtung der Daten.

Es bietet sich an, die gesamte Archivierung von Daten als Unternehmensprozess zu beschreiben. Für die sichere Vernichtung von Datenträgern existieren spezialisierte und diesbezüglich zertifizierte Unternehmen.

9.2 Vermeidung von Strafprozessen

In diesem Abschnitt betrachten wir Vorgehensweisen und Richtlinien, die der Vermeidung von Strafprozessen dienen und Tatbestände betreffen, die sich aufgrund des Verhaltens der Mitarbeiter gegenüber anderen Personen und durch Nutzung der Unternehmens-IT ergeben können. Dabei geht es nicht primär um *sensible* Daten des Unternehmens.

Unser erstes Thema beschäftigt sich mit der Vermeidung von Verleumdungen und übler Nachrede.

Verleumdung, üble Nachrede

Mitarbeitern ist explizit zu untersagen, beleidigende Äußerungen über Personen oder Organisationen zu verbreiten. Selbst wenn der eigentliche Inhalt der Wahrheit entspricht, können entsprechende Kommentare in Emails oder sonstigen Medien diffamierend sein. Die Folgen, gerade bei der Verbreitung über das Internet, können sehr ernst sein und erhebliche Strafen gegen das Unternehmen nach sich ziehen.

Copyright

Ein weiteres heikles Thema ist die Verwendung von geschütztem Material aus dem Internet. Bilder, Texte, Video-Clips, etc. aus dem Internet oder anderen elektronischen Quellen dürfen nicht ohne ausdrückliche Autorisierung durch den Eigentümer verwendet werden, selbst wenn dieses Material frei und ohne Einschränkung kopierbar ist. Das Copyright wird durch die massenweise Verbreitung über das Internet nicht aufgehoben. Ein Unternehmen kann sich strafbar machen, falls geschützte Inhalte

aus dem Internet im IT-Verbund des Unternehmens ohne Genehmigung des Urhebers gespeichert oder verarbeitet werden. Dies beinhaltet ebenfalls die elektronische Weiterverbreitung solcher Inhalte über Email oder Weblinks. Bei Verwendung von Texten aus Büchern, Reports oder anderen Dokumenten ist neben der Genehmigung zur Verwendung auf Korrektheit der Passagen und auf Gültigkeit innerhalb des betrachteten Kontextes zu achten.

9.3 Outsourcing

In diesem Abschnitt wollen wir uns rechtliche Rahmenbedingungen ansehen, die für den Bezug von IT-Dienstleistungen von externen Dienstleistern relevant sind.

Outsourcing

Unter Outsourcing verstehen wir die Beauftragung eines externen Dienstleisters mit Aufgaben der Datenverarbeitung. Beispiele dazu sind:

- Hardware (PC, Server) wird beim Dienstleister gemietet und von diesem gewartet.
- Das Netzwerk des Unternehmens mit Servern und Clients wird von einem externen Dienstleister betreut.
- Service-Center, Hotlines und User Help Desks werden von einem externen Dienstleister eingerichtet.
- Fernwartung wird vom Standort des Dienstleisters aus (remote) durchgeführt.
- Kundenbefragungen werden von einem externen Dienstleister durchgeführt.
- Klassische RZ-Dienste wie Monitoring, Job-Scheduling, Archiving und Backups werden vom Dienstleister übernommen.
- Application Hosting: SW-Anwendungen sowie damit verbundene Dienstleistungen werden über ein Netzwerk unter Abrechnung von Software-Lizenzen per erfolgter Nutzung zur Verfügung gestellt; als Stichwort zur plakativen Verdeutlichung sei hier „SAP aus der Steckdose“ genannt.
- Daten werden auf eigenen oder fremden Rechnern des externen Dienstleisters verarbeitet.

Outsourcing konfrontiert uns mit zwei Problemkreisen:

- Die eigentliche Vertragsgestaltung mit dem Ziel des möglichst reibungslosen Ablaufes im Tagesgeschäft.

Dazu gehören detaillierte Beschreibungen der vom Dienstleister zu erbringenden Dienstleistungen, und zwar unter Einbeziehung aller Sicherheitsaspekte – auch unter Extremsituationen (K-Fall).

– Outsourcing unter den Gesichtspunkten des Datenschutzes.

BDSG

Zwei Faktoren sind beim Outsourcing von erheblicher Wichtigkeit und Tragweite für die Einhaltung der datenschutzrechtlichen Bestimmungen:

– Der Standort des Dienstleisters: Datenschutzrechtlich können Probleme entstehen, wenn der Dienstleister seinen Firmensitz außerhalb der Europäischen Union, Norwegens, Islands und Liechtensteins hat, weil dann die dort geltenden Datenschutzbestimmungen nicht auf Deutschland übertragbar sein dürften.

– Die Weitergabe personenbezogener Daten an den Dienstleister: Bei der Vergabe der Lohn- und Gehaltsabrechnung an einen Dienstleister als Beispiel ist es zwingend notwendig, personenbezogene Daten an den Dienstleister weiterzugeben.

Eine im juristischen Sinne als *Übermittlung* anzusehende Weitergabe von personenbezogenen Daten setzt nach dem BDSG eine Erlaubnis sowie Informationspflichten voraus. Andernfalls ist die Übermittlung grundsätzlich verboten. Nicht *jede* Weitergabe von personenbezogenen Daten ist allerdings im juristischen Sinne automatisch als *Übermittlung* anzusehen:

Funktionsübertragung

Bekommt der Dienstleister im Rahmen des Outsourcing-Vertrages eine Funktion übertragen, sind von ihm alle Vorschriften des BDSG zu beachten. Der Dienstleister wird in diesem Fall vom Gesetz wie eine Fachabteilung des eigenen Unternehmens betrachtet, und es kann §11 BDSG angewendet werden. Hierzu muss in den Verträgen mit dem Dienstleister die Verpflichtung der Mitarbeiter des Dienstleisters auf das Datengeheimnis enthalten sein. Bei Verstößen im Umgang mit Daten durch den Dienstleister haftet das eigene Unternehmen, das den Outsourcing-Vertrag abgeschlossen hat. Die Einhaltung der datenschutzrechtlichen Pflichten hat der Auftraggeber zu prüfen. Auch Wartung gilt als Umgang mit Daten, da der Zugriff auf Daten durch das Wartungspersonal nicht ausgeschlossen werden kann. Neben dem BDSG kommen je nach Form der Beauftragung auch das Telekommunikationsgesetz (TKG), das Teledienstedatenschutzgesetz (TDDSG) und der Mediendienste-Staatsvertrag (MDStV) zur Anwendung. Eine Funktionsübertragung an einen Dienstleis-

ter ist daher rechtlich eine komplizierte Sache und sollte wenn irgend möglich vermieden werden.

Auftragsdatenverarbeitung

Wesentlich einfacher ist es hingegen, wenn dem Dienstleister eine Funktion nicht vollständig, sondern nur teilweise übertragen wird. Dabei handelt es sich rechtlich gesehen um eine *Auftragsdatenverarbeitung*, bei der keine personenbezogenen Daten „übermittelt", sondern nur für die Verarbeitung weitergegeben werden. Wichtig ist es dabei, eine klare Abgrenzung zur Funktionsübertragung zu finden, was in der Regel dadurch erreicht wird, dass die beauftragten Teile der Datenverarbeitung im Leistungskatalog klar aufgeführt werden. Es wird – um bei dem Beispiel von oben zu bleiben – keine Lohn- und Gehaltsabrechnung beauftragt, sondern einzelne Teile wie „Ermittlung der Bruttogehälter", „Ermittlung der anfallenden Lohnsteuer und Sozialversicherungsbeiträge" bis hin zum „Drucken und Kuvertieren der Gehaltsabrechnung".

9.4 Verschiedenes

In diesem Abschnitt diskutieren wir weitere in der Praxis vorkommende Ereignisse, die rechtliche Relevanz erlangen können.

Aufzeichnung von Sicherheitsverstößen

Ereignisse, die in irgendeiner Form die Informationssicherheit betreffen, lassen sich im Unternehmen nicht vermeiden. Alle Mitarbeiter haben aber darauf zu achten, dass erkannte, sicherheitsrelevante Ereignisse dokumentiert und an die für die Informationssicherheit verantwortlichen Stellen im Unternehmen weitergeleitet werden. Dabei sind zwei Fälle zu unterscheiden:

- Es gibt signifikante Anzeichen für einen bevorstehenden Verstoß gegen die Informationssicherheit.
- Ein Verstoß gegen die Informationssicherheit ist erfolgt.

Beweissicherung

Es ist wichtig, bereits die ersten Anzeichen einer Unregelmäßigkeit im Systemverhalten, Merkwürdigkeiten im Verhalten des Reinigungspersonals usw. zu dokumentieren. Wenn sich Verdachtsmomente auf eine Verletzung der Informationssicherheit verdichten, ist die Unternehmensleitung zu unterrichten, ggf. sind Ermittlungs- bzw. Aufsichtsbehörden hinzuzuziehen. Für die Sicherheitsleitlinie und deren Konkretisierung im Sicherheitskonzept sollte deshalb beachtet werden, dass

- unzulässige Beweise, verursacht durch eine unsachgemäße Dokumentation, ein entsprechendes Strafverfahren verhindern können,

- ein Mangel an Kontinuität und Vollständigkeit einer Beweiskette die eigene Position vor Gericht empfindlich schwächen kann,
- Beweise einer Überprüfung ihrer Integrität standhalten müssen, wenn sie nicht angezweifelt werden sollen,
- keine entsprechende Klage vom Unternehmen erhoben werden kann, wenn es keinen schriftlichen Beweis gibt, dass ein Eindringling Zugriffsrestriktionen zur Kenntnis genommen haben muss,
- Beweise vor Gericht für ungültig angesehen werden können, wenn keine schriftlich niedergelegten Prozeduren für Sammlung, Speicherung und Sicherung von Beweismaterial existieren.

Sammlung von verwertbarem Beweismaterial ist ein sehr schwieriges Unterfangen. Bei der Sammlung und Auswertung sollte man „forensische" Experten hinzuziehen.

Registrierung von Web-Domänen

Skizzieren wir als weiteres Thema die Registrierung von *Domain Names*. Registrierte Domänen für die Präsenz des Unternehmens im Internet gehören zu den schutzwürdigen Werten und Daten des Unternehmens. Falls die Kontrolle über diese Namen verloren geht, bedeutet das in den meisten Fällen den Verlust des Nutzens von Marketingmöglichkeiten. Alle auf dem Internet basierenden Vermarktungen, Angebote, etc. verlieren damit ihre Gültigkeit. Auch ermöglicht eine abgelaufene Registrierung Wettbewerbern, einen eingeführten und wohlbekannten Namen zu übernehmen.

Risikoversicherungen

Unser nächster Punkt betrifft Risikoversicherungen, die zur Überwälzung von Schäden auf Versicherungsunternehmen gebräuchlich sind. Dazu ist periodisch eine Risikoabschätzung durchzuführen, entsprechende Verträge sind mit den Versicherungen abzuschließen beziehungsweise zu erneuern. Versäumnisse, versicherbare Risiken durch Versicherungen abzudecken, können zu Haftungsklagen und hohen finanziellen Verlusten für das Unternehmen führen.

Aufzeichnen von Telefonaten

Nun kommen wir zu einem etwas delikaten Thema: der Aufzeichnung von Telefonaten. Es ist bei Hotlines, Supportcenter oder Telefonkonferenzen nicht unüblich, die Telefongespräche aus den verschiedensten Gründen aufzuzeichnen. Damit keine Persönlichkeitsrechte direkt verletzt werden, sind vor dem Start der Aufzeichnung alle Gesprächsteilnehmer darauf hinzuweisen, ihre Erlaubnis ist einzuholen. Gespräche können als Voice-Re-

cordings elektronisch gespeichert oder transkribiert werden. Unabhängig vom Verfahren dürfen Sie nur aufgezeichnet werden, wenn alle Teilnehmer damit einverstanden sind. Aufzeichnung von Telefongesprächen unterliegen dem Datenschutz und sind entsprechend gegen Verfälschung und nicht autorisierten Zugriff zu schützen.

Non-disclosure Agreements

Abschließen wollen wir dieses Kapitel mit dem Thema *Vertraulichkeitsvereinbarungen* (NDA, Non Disclosure Agreement) zwischen Firmen bzw. Kooperationspartnern. Es ist eine weit verbreitete Praxis, NDAs in die Verträge mit Partnern und Auftragnehmern aufzunehmen. NDAs haben dann ihre Berechtigung, wenn sensitive Informationen – im Sinne der Sicherheitsziele des Unternehmens – zwischen Partnern auf Zeit auszutauschen sind, die insbesondere nicht an Dritte weitergegeben werden dürfen – wie zum Beispiel Produkt- oder Preisinformationen. Werden keine NDAs vereinbart, besteht die Gefahr, dass sensitive Informationen z. B. an Wettbewerber weitergegeben werden. Dies gilt auch *nach* Beendigung des Kooperations- bzw. Auftragsverhältnisses, wenn das NDA keine diesbezüglichen Regelungen vorsieht.

10 Personelle Sicherheit

Ein ganz entscheidender Faktor zur Erreichung von Sicherheitszielen ist das Treffen von Maßnahmen zur Minimierung von Bedrohungen, welche von *berechtigten* Benutzern ausgehen. Die überwiegenden Schäden in Unternehmen – die aktuellen Statistiken weisen 60-85 % – werden von den eigenen Mitarbeitern und Fremdfirmenpersonal verursacht. Die Gründe dafür sind in der Regel vielfältig: Leichtsinn, Unachtsamkeit, Unkenntnis über die Implikationen des eigenen Verhaltens, ungezügelter Spieltrieb, Frustration und negative Motivation, selten auch kriminelle Motive, spielen eine dominante Rolle.

Social Engineering

Zusätzlich sind bei fehlender personeller Sicherheit Angriffe von außen über das so genannte Social Engineering sehr erfolgreich.

Nach ISO 27001 ist der Zweck der personellen Sicherheit die Reduzierung der Risiken, die durch menschliche Fehler, Diebstahl, Betrug und Missbrauch von Einrichtungen hervorgerufen werden. Entsprechend unterteilt sich die personelle Sicherheit in die Themenbereiche:

- Arbeitsverträge,
- Umgang mit vertraulichen Personaldaten,
- Verantwortung der Mitarbeiter für Erhaltung der Informationssicherheit,
- Personalmanagement,
- Vorkehrungen beim Ausscheiden von Mitarbeitern,
- Verschiedenes.

Wir werden in den nachfolgenden Abschnitten die einzelnen Themenbereiche mit Beispielen aus der Praxis behandeln.

10.1 Arbeitsverträge

Ein weites Feld ist die Gestaltung von Arbeitsverträgen unter dem Gesichtspunkt der Sicherheit. Wir unterscheiden dabei nicht zwischen zeitlich begrenzten und unbegrenzten Verträgen und schließen Verträge zur temporären Beschäftigung von Fremdfirmenpersonal ein. Wichtige Bestandteile von Arbeitsverträgen sind

- allgemeine Regelungen und Vereinbarungen,
- zusätzliche Klauseln für Personal von Fremdfirmen,
- Umgang mit Firmenlogos, Firmen-Emblemen, offiziellem Briefpapier, etc.,
- Umgang mit Berechtigungen,
- Gewähren von Krediten an Kollegen,
- Einverständnis mit der Sicherheitsleitlinie des Unternehmens,
- Regelungen über den Schutz geistigen Eigentums,
- Verantwortung des Mitarbeiters für die Geheimhaltung ihm zugänglicher Informationen.

Die oben aufgeführten Punkte sollten in einem Standardarbeitsvertrag enthalten sein. Abweichungen in Einzelfällen sind natürlich möglich und können durch Anhänge, Zusatzvermerke usw. geregelt werden. Was haben nun die aufgeführten (Mindest-) Bestandteile des Arbeitsvertrages mit dem Sicherheitsmanagement im Unternehmen zu tun? Beginnen wir mit den allgemeinen Regelungen und Vereinbarungen.

Allgemeine Regelungen und Vereinbarungen

Diese Regeln beschreiben die prinzipielle Art des Beschäftigungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer. Variiert wird dabei nur wenig, etwa in der Art der Organisation, der einzunehmenden Position und dem Verantwortungsbereich. Bereits hier sollte schon auf die Richtlinien zur Informationssicherheit des Unternehmens und deren Beachtung Bezug genommen werden. Fehlt diese Information, ist es nahe liegend, dass der Arbeitnehmer der irrigen Meinung unterliegt, er trage keinerlei Verantwortung für die Informationssicherheit. Auch werden beim Fehlen dieser Hinweise etwaige Schadensersatzklagen bei Verstössen erschwert.

Bei Verträgen mit Fremdfirmen muss unmissverständlich festgehalten werden, dass

- für die Dauer der Beschäftigung die eigenen Regeln für die Informationssicherheit gelten und
- alle Beschäftigten der Fremdfirma einschließlich etwaiger Unterauftragnehmer, die innerhalb des Vertrages für das Unternehmen tätig sind, diese Regeln zu beachten haben.

Vor Unterzeichnung des Vertrages ist der Fremdfirma ein Exemplar der zu beachtenden Sicherheitsgrundsätze auszuhändigen oder anderweitig zugänglich zu machen (z. B. über die Home-

page des Unternehmens). Es reicht in der Regel nicht aus, auf Informationschutzrichtlinien der Fremdfirmen zu vertrauen.

Umgang mit Firmenlogos

Ein weiterer wichtiger Bestandteil des Arbeitsvertrages betrifft den Umgang mit Firmenlogos, Firmenemblemen, etc. Firmenlogos wird häufig zu unrecht die Funktion eines Echtheitsnachweises zugeordnet. Sie werden als Authentisierungsmerkmal angesehen und können als solches missbraucht werden. Dementsprechend muss in den Arbeitsverträgen der Umgang mit ihnen geregelt werden. Die Schädigung der Reputation und des Ansehens des Unternehmens durch Missbrauch von Firmenlogos auf Briefpapier, in Emails etc. kann bei Fehlen einer entsprechenden Regelung kaum geahndet werden.

Authentifizierungsmerkmale

Als nächsten Punkt betrachten wir die Weitergabe von Authentisierungsmerkmalen wie Werksausweise, Passwörter, Tokens usw. an andere Personen, wobei hier nicht zwischen Mitarbeitern im gleichen Unternehmen (Kollegen) und Außenstehenden unterschieden wird. Es muss im Arbeitsvertrag unmissverständlich und explizit verboten sein, Authentisierungsmerkmale an andere Personen weiterzugeben, da durch diese Handlung die Sicherheitsfunktion *Authentisierung* konterkariert wird und alle Prozesse, die auf der Authentisierung aufbauen, unsicher werden.

Kredite und Darlehen

Es mag sich vielleicht zunächst seltsam lesen, aber eine Regelung über die Gewährung von Krediten[42] an Kollegen gehört ebenfalls in den Vertrag. Der Grund ist, dass das Einräumen von Krediten gegenüber Kollegen früher oder später zu einem schlechten Betriebsklima, Interessenskonflikten beispielsweise bei anstehenden Beförderungen und zur Anwendung von Repressalien führen kann – Tatbestände, die auch für die Informationssicherheit eine Bedeutung haben können. Die Gewährung von Krediten für Mitarbeiter im Unternehmen sollte streng untersagt sein.

Einverständnis mit Sicherheitsrichtlinien

In den Arbeitsvertrag gehört auch eine Einverständniserklärung mit den Richtlinien[43] zur Informationssicherheit des Unternehmens. Diese Richtlinien müssen in leicht lesbarer Form (Home-Page, Ausdruck, PDF-Dokument auf einer CD, etc.) dem potenziellen Mitarbeiter vor Unterzeichnen des Vertrages zugänglich

---

[42] Damit ist nicht das Auslegen eines Mittagessens wegen einer vergessenen Brieftasche gemeint, sondern das Verleihen von Geld gegen Zinsen.

[43] die IT-Sicherheitspolitik und ggf. weitere Dokumente

gemacht werden. Im Vertrag sollte sich ein Passus befinden, nach dem der Mitarbeiter mit Unterzeichnung des Vertrages erklärt, die Sicherheitsrichtlinien erhalten, zur Kenntnis genommen und verstanden zu haben und sie in seinem Beschäftigungsverhältnis zu beachten. Auch sollte im Vertrag darauf hingewiesen werden, dass Sicherheitsvorfälle, die aufgrund der Nichtbeachtung von Sicherheitsrichtlinien durch den Mitarbeiter herbeigeführt wurden, unmittelbar disziplinarische Maßnahmen nach sich ziehen kann.

Schutz geistigen Eigentums

Der vorletzte Punkt der eingangs angeführten Bestandteile des Arbeitsvertrages betrifft den Schutz des geistigen Eigentums. In diesem Vertragsteil wird die Eigentümerschaft von Patenten, Forschungsergebnissen, Publikationen, etc., geregelt. Das geistige Eigentum, das aus Tätigkeiten im und für das Unternehmen resultiert, liegt beim Unternehmen. Dies gilt auch für Personal von Fremdfirmen und anderen Vertragspartnern, die im Auftrag des Unternehmens bestimmte Gewerke erstellen oder Tätigkeiten ausüben. Abweichungen, beispielsweise bei Patenten, können vorkommen und müssen gesondert betrachtet werden (Anhänge, Beiblätter, etc.).

Schutz vertraulicher Informationen

Kommen wir zum letzten Punkt, der Verantwortung der Mitarbeiter zum Schutz vertraulicher Informationen des Unternehmens. Neben der Anerkennung der Informationsschutzrichtlinien des Unternehmens gehört auch die Einverständniserklärung des Mitarbeiters mit der von ihm erwarteten Eigenverantwortung zum Schutz vertraulicher Informationen zum Arbeitsvertrag. Diese Erklärung gilt in der Regel auch für eine bestimmte Frist nach dem Ausscheiden aus dem Unternehmen. Damit soll vermieden werden, dass

- vertrauliche Informationen an Dritte weitergegeben werden,
- bei Wechsel des Mitarbeiters zu einem Wettbewerber keine vertraulichen Informationen als „Morgengabe“ mitgebracht werden,
- Mitarbeiter über ihre Verantwortung bei der nicht autorisierten Weitergabe sensitiver Informationen im Unklaren gelassen werden,
- vertrauliche Informationen nur mit befugten Kollegen und nur an Arbeitsplätzen ohne Mithörmöglichkeit diskutiert werden.

10.2 Vertrauliche Personaldaten

Nach der Gestaltung der Arbeitsverträge wenden wir uns dem Umgang mit personenbezogenen Daten zu. Bei der Regelung dieser Daten befinden wir uns in dem Spannungsfeld zwischen entsprechenden Gesetzen (Datenschutzgesetz, Fernmeldegesetz, etc.) sowie dem Schutz der Privatsphäre des Mitarbeiters und den Interessen des Unternehmens. Wir teilen diesen Abschnitt in folgende Bestandteile auf:

- Respektierung der Privatsphäre am Arbeitsplatz,
- Umgang mit vertraulichen Personaldaten,
- Erstellung von Arbeitszeugnissen, Referenzen, etc.,
- Überprüfung der Sicherheitseinstufung („Clearance“) von Mitarbeitern,
- Austausch von Personalinformationen mit anderen Mitarbeitern.

Schutz der Privatsphäre

Beginnen wir mit der Beachtung der Privatsphäre der Mitarbeiter, die je nach Land durch entsprechende Gesetze (in Deutschland durch das Datenschutzgesetz, das Telekommunikationsgesetz usw.) geregelt ist. Die Inhalte dieser Gesetze sind natürlich von der Unternehmensleitung zu beachten. Prinzipiell hat die Unternehmensleitung das Recht auf Zugriff zu allen Informationen, die im IT-Verbund des Unternehmens erzeugt oder gespeichert werden.

Was von dieser Regelung ausgenommen und zu der Privatsphäre des Mitarbeiters gezählt wird, muss explizit und eindeutig geregelt werden. Beispielsweise kann ein privates elektronisches Telefonbuch vom Arbeitgeber auf einem dienstlichen Notebook geduldet und zu der Privatsphäre des Mitarbeiters gezählt werden. Wird eine solche Festlegung bzw. Regelung jedoch unterlassen, kann der Arbeitnehmer der irrigen Annahme sein, dass alles erlaubt ist und zum Beispiel auch rechtsradikales Gedankengut in Wort und Bild speichern, was bei Audits und anderen Sicherheitsüberprüfungen Ärger verursachen, generell Rufschädigung und teure Prozesse nach sich ziehen kann.

Beim Umgang mit Personaldaten ist generell auf strikte Wahrung der Vertraulichkeit zu achten. Sie dürfen nur einem ausdrücklich und nachprüfbar autorisierten Personenkreis zugänglich gemacht werden. Auf peinlich genaue Einhaltung der einschlägigen Gesetze ist zu achten. Bei Nichteinhaltung drohen neben Reputationsverlust hohe Geld- und Haftstrafen.

Dienstzeugnisse Jeder Mitarbeiter hat das Recht, ein Dienstzeugnis oder eine Referenz von seinem Arbeitgeber zu erhalten. In diesen Fällen ist darauf zu achten, dass der Anlass dokumentiert wird und die gewünschten Dokumente nur von autorisierten Personen ausgestellt werden. Hier besteht eine Querverbindung zu der zuvor angeführten notwendigen Regelung zur Verwendung offizieller Firmenstempel oder Logos: Nur die autorisierten Personen dürfen die gewünschten Referenzen auf offiziellem Firmenpapier ausstellen. Wer solche Dokumente unterschreiben darf, ist Bestandteil der allgemeinen Unterschriftenregelung.

Personalauswahl Wie eingangs angeführt, führen Sicherheitsvorfälle im Zusammenhang mit autorisierten Mitarbeitern („Befugte") die Schadenstatistik an. Deshalb sind bei der Personalauswahl für Mitarbeiter, die in sensiblen Bereichen des IT-Verbunds des Unternehmens eingesetzt werden sollen, hohe Maßstäbe an Charakter und Integrität, d. h. an die Vertrauenswürdigkeit anzulegen.

Sicherheitsüberprüfung In besonders sensitiven Bereichen greift man zu einer formellen *Sicherheitsüberprüfung*, die ggf. unter Einbeziehung von Behörden eine rückschauende Einschätzung der Vertrauenswürdigkeit einer Person liefert. Dabei kann z. B. ein polizeiliches Führungszeugnis oder eine Ermächtigung für behördliche Verschlusssachen das Ziel sein.

In der Regel werden sensible Tätigkeiten in möglichst wenigen *Rollen* beschrieben und den dafür ausgewählten Mitarbeitern zugewiesen. Diese Zuweisung muss periodisch auf Angemessenheit für die ausgeübte Tätigkeit und auf persönliche Eignung überprüft werden. Ein langjähriger Administrator einer sensiblen Applikation, der z. B. durch ein schweres familiäres Schicksal zum Alkoholiker wurde, ist zur Ausübung der ursprünglich zugewiesenen Rolle nicht weiter geeignet.

Eine Rolle kann Aufgaben und Berechtigungen beinhalten, die z. B. durch technische Änderungen der Infrastruktur obsolet werden. Hier muss entschieden werden,

- ob die Rolle weiter nötig ist,
- ob eventuell andere existierende Rollen die verbleibenden Aufgaben übernehmen können.

Generell gilt hier das Prinzip „Weniger ist mehr". Ein „Mehr" erreicht man hier hinsichtlich der Überprüfbarkeit bzw. der Auditierungsfähigkeit.

Austausch von Informationen

Kommen wir zu der Weitergabe von persönlichen Informationen über Mitarbeiter durch Mitarbeiter, hier insbesondere Gerüchte über Beförderung, Degradierung, Entlassung, Gehalt, usw. von Kollegen. In aller Regel sollte die Weitergabe von Gehaltsdaten explizit in Arbeitsverträgen untersagt werden. Gerüchte über Beförderung, Degradierung, Entlassung, usw. sind nie ganz zu unterbinden. Es sollte aber eine unmissverständliche Anweisung publiziert werden, dass solche Informationen – sofern solche überhaupt veröffentlicht werden dürfen – nur als authentisch anzusehen sind, wenn sie von einer benannten Stelle kommen, z. B. von der Einheit „Communications" des Unternehmens. Toleriert man die „Gerüchteküche" mit nicht autorisierten Informationen über Mitarbeiter,

- kann sich eine Verschlechterung des Betriebsklimas einstellen, das seinerseits negative Auswirkung auf die Disziplin der Mitarbeiter (aus Enttäuschung, Unzufriedenheit, etc.) und damit auf die Sicherheit haben kann,
- können auch unerwünschte Rechtstreitigkeiten die Folge sein.

10.3 Verantwortung der Mitarbeiter für die Informationssicherheit

Oft ist es den Mitarbeitern nicht bewusst, welche Eigenverantwortung zur Informationssicherheit ihnen übertragen wurde. Zur Vermeidung von Missverständnissen müssen entsprechende Regelungen erlassen werden und dem Mitarbeiter bekannt sein. Wir wollen exemplarisch einige wichtige Themen aus diesem Bereich aufführen und diskutieren:

- Verwendung der Firmenzugänge zum Internet,
- Geheimhaltung von Passwörtern und PINs,
- Verwendung von Email und Telefonie,
- Umgang mit Firmen-Kreditkarten,
- Bestellung von Waren und Dienstleistungen, Bestätigung von Lieferungen und Leistungen, Bestätigung von Rechnungen,
- Weitergabe von Geräten und vertraulichen Informationen an Familienmitglieder,
- Private Verwendung der unternehmenseigenen PC, Notebooks, etc.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit. Es sind entsprechend der Art der Geschäftstätigkeit und den betrieblichen Belangen weitere Punkte aufzunehmen.

Internet-Zugänge

Beginnen wir mit der betrieblichen Verwendung der firmeneigenen Internet-Zugänge. Hier ist zu regeln, auf welches Material *nicht* zugegriffen werden darf: z. B. auf Webseiten und Daten mit rassistischem und pornografischem Material, illegale Kopien aus Tauschbörsen wie eDonkey und BitTorrent, Chat-Räume, Online-Spiele, News Groups, soweit diese keinen Bezug zur betrieblichen Tätigkeit aufweisen. Entsprechend der Gesetzeslage in Deutschland sind Überprüfungen des Nutzungsverhaltens nur im Rahmen von Ermittlungen und nach Absprache mit den zuständigen Stellen und der Mitarbeitervertretung zulässig.

Prinzipiell muss der Download von Software und die Installation derselben auf dem firmeneigenen PC untersagt werden.

Neben technischen Möglichkeiten zur Einschränkung des Zugriffs auf das Internet führt hier nur konsequente Sensibilisierung und Schulung der Mitarbeiter weiter. Der Disziplinar-Prozess bei Zuwiderhandlung muss ebenfalls allen Mitarbeitern bekannt sein.

Passwörter und PINs

Passwörter, PINs und andere Authentisierungsmerkmale werden immer dann verwendet, wenn der Zugriff auf Informationen auf einen bestimmten Benutzerkreis eingeschränkt ist und die entsprechenden Informationen nicht jedem zugänglich gemacht werden dürfen. Sie sind unbedingt vertraulich zu behandeln. Entsprechende Regelungen müssen erlassen und kommuniziert sein. Die nicht autorisierte Weitergabe solcher Authentisierungsmerkmale – gleich, ob an Externe oder Mitarbeiter – ist disziplinarisch zu ahnden.

Analog gilt dies grundsätzlich für die Weitergabe *jeder* Art vertraulicher Informationen an Kollegen. Informationen werden auch dann kompromittiert, wenn sie Mitarbeitern des *gleichen* Unternehmens zugänglich gemacht werden, ohne dass diese eine diesbezügliche Autorisierung besitzen.

Email und Telefonie

Die Verwendung des Email-Systems sowie des dienstlichen Telefons (Mobil- und Festnetz) für private Zwecke lässt sich nicht ganz unterbinden. Es muss aber explizit darauf hingewiesen werden, dass der Gebrauch nur in Notfällen gestattet ist, um einem exzessiven Gebrauch dieser Infrastruktur mit den damit verbundenen Kosten und der Einschränkung der Bandbreite vorzubeugen.

Kreditkarten

Für Kreditkarten, Tankkarten, Servicekarten etc., die auf das Unternehmen ausgestellt sind und autorisierten Mitarbeitern ausgehändigt werden, sind Regelungen für folgende Punkte in Betracht zu ziehen:

- Vorgehen bei Diebstahl oder Verlust,
- Weitergabe der Kartendaten über das Internet,
- Kontrolle der Kartenabrechnung,
- Weitergabe an Dritte.

Bestellungen, Lieferungen und Rechnungen

Ein weiterer wichtiger Punkt der Eigenverantwortung des Mitarbeiters ist die strikte Einhaltung der Prozesse des Unternehmens beim Auslösen von Bestellvorgängen, dem Empfang und der Anerkennung von Lieferungen und Leistungen und der Bestätigung von Rechnungen. Die entsprechenden Prozesse müssen in Regelwerken niedergelegt und den Mitarbeitern bekannt sein. Beim Empfang von Waren und Services oder bei dem Bestätigen von Rechnungen besteht beispielsweise die Gefahr, dass nicht autorisierte Personen Zugang zu sensitiven Bereichen des IT-Verbunds des Unternehmens erhalten. Bei der Bestätigung von Rechnungen durch nicht autorisierte Mitarbeiter können spätere Reklamationen nicht oder nur unter Schwierigkeiten geltend gemacht werden.

Familienmitglieder

Ein heikles Thema ist die Weitergabe mobiler Endgeräte und ggf. vertraulicher Informationen des Unternehmens an Familienmitglieder. Mitarbeiter sind darauf hinzuweisen, dass technische Einrichtungen zur Wahrnehmung betrieblicher Tätigkeiten wie Smartphones, Organizer, Notebooks, um nur einige zu nennen, nicht in die Hände von Familienmitgliedern gehören. Diese Vorgabe kann bis zum generellen Verbot der privaten Nutzung unternehmenseigener Technik *zu Hause* reichen. Mit einer solchen Regelung lässt sich unter anderem die Gefahr des Einbringens maligner (bösartiger) Software wie Computerviren, Trojaner und Computerwürmer in die Infrastruktur des Unternehmens verringern.

Es liegt in unserer Natur, Ereignisse und Erlebnisse aus der beruflichen Tätigkeit in einem Unternehmen mit den Mitgliedern der eigenen Familie zu diskutieren. Die Familie wird immer noch als ein Ort der Vertrautheit und Intimität angesehen. Man sollte sich jedoch davor hüten, Vertrautheit mit Vertraulichkeit gleichzusetzen. Familienmitglieder sind sich oft auch nach eindringlicher Warnung der Brisanz und Sensibilität von Unternehmensinformationen nicht bewusst und geben sie ohne Argwohn bei

passender Gelegenheit an Dritte weiter („Kindermund tut Wahrheit kund"). Es muss deshalb explizit beim Umgang mit vertraulichen Informationen darauf hingewiesen werden, dass diese Informationen auch nicht an Mitglieder der eigenen Familie weitergegeben werden dürfen. Es ist insbesondere darauf zu achten, dass Sicherheitsvorkehrungen wie Verschlüsselung, die strikte Befolgung der Clean Desktop Policy usw. auch beim Home Office eingehalten werden.

10.4 Personalmanagement

Wir wollen in diesem Abschnitt folgende Punkte näher betrachten:

- Umgang mit enttäuschten, demotivierten Mitarbeitern,
- Handhabung von vertraulichen Gesprächsnotizen.

Enttäuschte Mitarbeiter stellen gerade heute in den Zeiten großflächigen Personalabbaus und von Umstrukturierungen ein nicht unerhebliches Risiko dar. Das Risiko ist auch unter dem Aspekt gravierend, dass es sich bei demotivierten Mitarbeitern oft kurz zuvor noch um vertrauenswürdige Mitarbeiter handelte, die mit entsprechenden Befugnissen und Rechten ausgestattet waren. Dem Mitarbeiter ist es in der Regel nicht anzumerken, wann sich der Wandel vom loyalen Firmenangehörigen zur Bedrohung für die Informationssicherheit vollzieht. Zur Minimierung dieses Risiko sollten alle Anzeichen auf eine Verschlechterung des Arbeitsumfeldes und Enttäuschung bei den Mitarbeitern ernst genommen und offen kommuniziert werden.

Eine Ursache für eine negative Veränderung des Betriebsklimas kann z. B. die Verbreitung von Inhalten aus Personalgesprächen sein. Bei Personalgesprächen, Zielvereinbarungen etc. werden vom Vorgesetzten in der Regel Aufzeichnungen angefertigt. Diese unterliegen dem Datenschutzgesetz und sind streng vertraulich zu behandeln. Insbesondere dürfen sie nicht unberechtigten Dritten zugänglich sein.

10.5 Ausscheiden von Mitarbeitern

In diesem Abschnitt betrachten wir

- die Handhabung von Kündigungen, Pensionierungen, etc.,
- die Prozeduren nach erfolgter Kündigung,
- Vereinbarungen bei Wechsel zu einem Wettbewerber.

Wenn Mitarbeiter, aus welchen Gründen auch immer, das Unternehmen verlassen, muss frühestmöglich das Sicherheitsmanagement davon in Kenntnis gesetzt werden. Es hat gemeinsam mit dem disziplinarischen Vorgesetzten das Risiko abzuschätzen, das entsteht, wenn der ausscheidende Mitarbeiter bis zu seinem endgültigen Austritt weiterhin die ihm übertragenen Rechte auf Zugriff zu Informationen ausnutzen kann. Verläuft die Trennung harmonisch, so ist in der Regel das Risiko innerhalb der Zeitspanne vom Bekanntwerden der Entscheidung bis zum Verlassen des Unternehmens gering. Bei Trennungen bzw. Kündigungen, die nicht einvernehmlich erfolgen, sollte den Mitarbeitern der Zugriff auf sensible Daten des Unternehmens umgehend entzogen werden. In solchen Fällen können Regelungen, die die sofortige Übergabe des Arbeitsplatzes und anschließende Beurlaubung des Mitarbeiters bis zum endgültigen Ausscheiden aus dem Unternehmen, vorsehen, sehr hilfreich sein. Andernfalls besteht weiterhin das Risiko, dass vertrauliche Daten für private Zwecke kopiert oder aus Unzufriedenheit über die Trennung vom Unternehmen sabotiert werden.

Der letzte Punkt dieses Abschnitts spricht die häufig auftretende Situation an, dass der ausscheidende Mitarbeiter zu einem Wettbewerber des Unternehmens wechselt. Zur Vorbeugung der Übertragung von Know How auf die neue Arbeitsstelle werden meist Wettbewerbsklauseln in die Arbeitsverträge aufgenommen. Beispielsweise werden Fristen von mehreren Jahren vereinbart, in denen der Mitarbeiter nicht in einer gleichartigen Position beim Wettbewerber arbeiten darf, oder es werden lange Kündigungsfristen vereinbart, in denen der Mitarbeiter beurlaubt wird.

Solche Regelungen lassen sich jedoch meist umgehen, und ihre Einhaltung ist schwer zu kontrollieren. Auch besteht oft Rechtsunsicherheit, was in den Arbeitsverträgen überhaupt geregelt werden darf. Als Minimalforderung sollte jedoch die Behandlung sensibler Informationen in den Arbeitsverträgen geregelt werden.

11 Technische Sicherheitsmaßnahmen

Im Abschnitt über die Validierung von Sicherheitsmaßnahmen haben wir bereits eine grobe Einteilung möglicher Sicherheitsmaßnahmen nach

- vertraglichen und organisatorischen Regelungen sowie personellen Maßnahmen und
- mehr technisch ausgerichteten Infrastruktur- und IT-Maßnahmen („Sicherheitsfunktionen")

vorgenommen und im Kapitel „4. Sicherheitsziele auf allen Ebenen" Beispiele zu einzelnen Sicherheitsmaßnahmen kennen gelernt. Hier wollen wir jetzt einige ausgewählte technische Sicherheitsmaßnahmen näher behandeln. Dabei stellen wir jeder Maßnahme die Bedrohungen gegenüber, die sie abwehren bzw. deren Schadenauswirkung sie begrenzen soll.

Alle Sicherheitsmaßnahmen besitzen nicht nur einen „Wirkanteil", sondern haben stets auch einen Management-Anteil, mit dem wichtige „Einstellungen" vorgenommen oder Rahmenbedingungen gesetzt werden. Wir stellen deshalb im Folgenden neben der Funktion auch jeweils die Management-Aufgabe dar.

11.1 Wahrung der Vertraulichkeit

Die Forderung nach Vertraulichkeit hat zur Konsequenz, dass bei der Verarbeitung entsprechender Daten eine Zugriffskontrolle vorhanden sein muss: Sie unterscheidet anhand von entsprechenden Vorgaben Befugte von Unbefugten – was allerdings nur Sinn macht, wenn Personen zuverlässig identifiziert und authentisiert werden können. Wahrung der Vertraulichkeit erreichen wir folglich durch die Funktionen „Identifizierung und Authentisierung" und „Zugriffskontrolle", die man allerdings auf sehr unterschiedliche Weise realisieren kann. Diese und einige damit zusammenhängende Funktionen behandeln wir in den folgenden Abschnitten.

11.2 Identifizierung und Authentisierung

Diese beiden Funktionen treten fast immer in Kombination auf.

Identifizierung Als „Identifizierung“ bezeichnen wir zunächst die Funktion, die Identität eines Subjektes anzugeben. Typische Beispiele für Verfahren zur Identifizierung von Personen sind die Abfrage der User-ID am Terminal eines Rechners oder das *Vorzeigen* eines Ausweises bei einer Torkontrolle (ohne *Überprüfung* des Ausweises).

Management Soll in (IV-, IT-)Systemen eine Identifizierung stattfinden, stellen sich folgende Fragen:

- Welche Subjekte sollen identifiziert werden?
- Wodurch soll die Identifizierung erfolgen (Nennung des Namens, Vorzeigen des Ausweises, …)?
- Wie wird die Eindeutigkeit bei Namensgleichheit sichergestellt?
- Wie können in der Liste der Identitäten neue Identitäten hinzugefügt, bestehende geändert oder gelöscht werden?

Authentisierung Die Prüfung, ob eine angegebene Identität für ein Subjekt tatsächlich zutrifft, ist Aufgabe der Funktion „Authentisierung“. Diese Funktion kann sehr unterschiedlich realisiert sein:

- Sie tritt sehr oft in direkter Einheit mit der Identifizierung auf: Nach der Eingabe der User-ID bei einem Rechner wird ein Passwort abgefragt, dessen Kenntnis als Nachweis der Identität dient.
- Andere Verfahren der Authentisierung – etwa unter Nutzung von Smartcards – bedienen sich einer PIN oder biometrischer Daten.
- Die Ausweisprüfung (Handelt es sich um einen „echten“ Ausweis? Stimmt das Foto mit dem Subjekt überein?) ist ebenfalls eine Form der Authentisierung.

Vielfach wird die Authentisierung nach der Identifizierung ablaufen. Es ist aber durchaus denkbar, dass Identifizierung und Authentisierung praktisch zusammenfallen: Die Kenntnis eines bestimmten Geheimnisses (Passwort, PIN, Schlüssel) kann Befugte „auszeichnen“: Sie würden sich durch Angabe dieses Codes gleichzeitig identifizieren und authentisieren. Eine separate Angabe der Identität kann ggf. entfallen.

Eine Authentisierung kann grundsätzlich nur dann unterbleiben, wenn eine fehlerhafte Identifizierung ausgeschlossen werden kann. Dies ist z. B. denkbar, wenn die eigentliche Authentisierung bereits im Umfeld eines IT-Systems durchgeführt wurde

(etwa durch eine Ausweiskontrolle) und die Person an dem IT-System lediglich ihren Namen angibt, um ihre Arbeitsumgebung in dem IT-System zugewiesen zu bekommen. Hierbei wäre aber zu unterstellen, dass die Person vertrauenswürdig ist und sich nicht anderer Identitäten „bedient".

In der Praxis geht es aber immer darum, Befugten bestimmte Aktionen zu erlauben, Unbefugte dagegen „fernzuhalten". Mit der Funktion „Authentisierung" wird die angegebene Identität eines Subjektes geprüft, als korrekt bestätigt oder als nicht zutreffend erkannt. Ohne die Funktion der Authentisierung kann keine vernünftige Zugriffskontrolle und auch keine beweiskräftige Protokollierung durchgeführt werden.

Generell teilt man Authentisierungsverfahren wie folgt ein: Authentisierung durch

- Besitz eines Gegenstandes, z. B. eines (physischen) Schlüssels, einer Smartcard, eines Tokens, eines Ausweises,
- Wissen (Kenntnis) bestimmter Informationen, z. B. Passwort, PIN, Schlüssel,
- charakteristische Merkmale von Personen, z. B. biometrische Merkmale wie Retina- und Stimmenmuster, Fingerabdruck, Gesicht (Foto).

Bei der Authentisierung durch *Besitz* sind Authentisierungsmittel (Smartcards, Tokens, Ausweise) zu erzeugen und auszugeben, ggf. auch wieder zu entziehen. Dieser Prozess erfordert meist eine straffe Organisation und ist in großen Unternehmen eine nicht zu unterschätzende Aufgabe. Bei der Beurteilung der Stärke der Authentisierung durch Besitz sind die Möglichkeiten zum Entwenden des Gegenstandes und der Aufwand zum Fälschen bzw. Duplizieren dieses Gegenstandes zu untersuchen.

Im Fall der Authentisierung durch *Wissen* müssen die Möglichkeiten und der Aufwand zur Erlangung des Wissens durch Unbefugte diskutiert werden. Bleibt die Erzeugung der Wissensdaten (bspw. Passwörter, PINs) den Personen selbst vorbehalten, wird man Regeln zur Herstellung „guter" Passwörter oder PINs erlassen.

Bei der dritten Variante – Authentisierung durch *charakteristische Merkmale* – muss sehr genau überlegt werden, ob das vorgesehene Merkmal tatsächlich eine präzise Authentisierung der Person erlaubt: Wie hoch ist die Wahrscheinlichkeit, dass andere Personen für die „echte" Person gehalten werden können? Aber

auch: Wie hoch ist die Wahrscheinlichkeit, dass die „echte“ Person nicht erkannt wird? Wie hoch ist ggf. der Aufwand zum Fälschen der Merkmale und würden diese ggf. als Fälschung erkannt? Bei dieser Variante ist für einen flächendeckenden Roll-Out zu bedenken, dass die charakteristischen Merkmale zunächst erfasst werden müssen.

Die oben genannten Arten der Authentisierung treten oft in Kombination auf: Bei der Ausweisprüfung geht es um den Besitz eines (echten) Ausweises, aber auch um die Übereinstimmung zwischen Foto und Person (charakteristisches Merkmal). Bei der Nutzung von Smartcards als Authentisierungsmittel hat man den Besitz dieser Smartcard und die Kenntnis der PIN kombiniert (Besitz und Wissen). Spezielle Karten erlauben sogar, alternativ zur PIN oder zusätzlich zur PIN einen Fingerabdruck zu erfassen und mit dem gespeicherten Muster zu vergleichen.

Die Sicherheitsfunktionen Identifikation und Authentisierung sind selbst einer Reihe denkbarer Attacken ausgesetzt:

Spoofing

Der Vorgang der Identifizierung und Authentisierung kann durch Dritte beobachtet werden, und zwar physisch durch Zuschauen, aber auch durch Abhören und Abfangen von Identifikations- und Authentisierungsdaten mittels eines *Spoofing*-Programms.

Vertrauenswürdiger Kanal

In diesem Fall ist also die Kommunikation zwischen Subjekt und System nicht vertrauenswürdig. Anders ausgedrückt: Bei der Authentisierung benötigt man einen „vertrauenswürdigen“ Kanal zwischen Subjekt und System. Diese Überlegung führt im organisatorischen Bereich zur Regel, die Eingabe von Passwörtern verdeckt durchzuführen, im technischen Bereich beispielsweise zur Vorgabe an die Systementwickler, einen vertrauenswürdigen Kanal zwischen Tastatur zur Passwort-Eingabe und der das Passwort prüfenden Software einzurichten, um ein Abhören durch andere Prozesse zu verhindern.

Management

Aus Management-Sicht ist festzulegen:

- Bei welchen Anlässen ist eine Authentisierung durchzuführen?
- Welche Subjekte sollen authentisiert werden?
- Welches Verfahren der Authentisierung wird angewendet?
- Wann ist eine Authentisierung als erfolgreich anzusehen?
- Welche Aktionen werden bei nicht erfolgreicher Authentisierung ergriffen? Hierzu gehören auch Verfahren zur Begrenzung der Anzahl möglicher Authentisierungsversuche.

– Wie wird die Vertraulichkeit der Authentisierungsdaten gewährleistet?

Verwendet man eine Authentisierung durch „Wissen“, geht es immer darum, die Vertraulichkeit des „Geheimnisses“ sicherzustellen. Dies hat zur Folge, dass eine organisatorische Regel erlassen wird, Passwörter möglichst nicht aufzuschreiben; in technischen Systemen müssen Passwort-Listen gegen Auslesen geschützt werden.

– Wie wird die Integrität der Authentisierungsdaten gewährleistet?

Besonders in technischen Systemen hätte man als Hacker leichtes Spiel, wenn es möglich wäre, Passwort-Listen beliebig abzuändern.

– Wie wird die Verfügbarkeit der Authentisierungsdaten gewährleistet?

Werden in technischen Systemen Passwort-Listen versehentlich oder absichtlich gelöscht oder z. B. durch technischen Defekt zerstört oder anderweitig blockiert, ist keine Authentisierung mehr möglich – der Betrieb steht. Werden beispielsweise Admin-Passwörter aufgeschrieben und in einem Tresor aufbewahrt, muss ein Zugriff durch Befugte jederzeit möglich sein. Andernfalls können wichtige Administrationsarbeiten nicht durchgeführt werden.

Bisher haben wir die Authentisierung im Sinne von „Subjekt authentisiert sich an einem System“ betrachtet. Der umgekehrte Fall kann ebenfalls Sinn machen, wenn z. B. in einem Netzwerk ein Nutzer sicher sein möchte, mit welchem IT-System er in Verbindung steht. Hierfür führt man z. B. Server-Zertifikate ein, mit denen sich ein Rechner „ausweisen“ kann (s. Abschnitt „Elektronische Identität und deren Prüfung“).

Peer Entity Authentication

Eine weitere Form der Authentisierung ist die *Partner-Authentisierung* (*Peer Entity Authentication*). Hier wird der wichtige Aspekt herausgestellt, dass sich die Kommunikationspartner in einem Netzwerk *gegenseitig* authentisieren. Dies lässt sich z. B. durch die Verwendung elektronisch signierter Zertifikate erreichen, wenn diese „sicher“ an eine Person gebunden sind. Letzteres zu erreichen ist eine Aufgabe der so genannten „Registrierung“, der im Zusammenhang mit dem Signaturgesetz eine

besondere Bedeutung zukommt (s. Abschnitt „Elektronische Identität und deren Prüfung“).

Data Origin Authentication

Bei der Sicherheit von Geschäftsprozessen haben wir bereits das Thema der Verbindlichkeit der Kommunikation zwischen Partnern diskutiert. Bei der Kommunikation in einem Netzwerk geht es dabei auch darum, dass der Empfänger den Sender von Daten sicher identifizieren und authentisieren kann, damit dieser später seine Urheberschaft nicht leugnen kann.

11.3 Zugriffskontrolle

Erst wenn Subjekte identifiziert und authentisiert worden sind, kann entschieden werden, ob ihnen die gewünschte Aktion gestattet werden darf.

Zugriffskontrolle

Durch die Zugriffskontrolle wird überprüft, ob ein bestimmtes Subjekt berechtigt ist, eine gewünschte Aktion mit einem Objekt auszuführen. Als Aktionen kommen u. a. das Erzeugen, Lesen, Ändern und Löschen von Daten in Frage – im Grunde alle im Abschnitt „Grundstrukturen“ genannten „Verarbeitungen“.

In einem IT-System wird man für die Zugriffskontrolle das Betriebssystem einsetzen. Hier haben wir eine zentrale Zugriffskontrolle. Außerhalb von IT-Systemen realisiert man Zugriffskontrolle z. B. durch

- Vergabe und Management physischer Schlüssel: Zugang zu Räumen, Zugriff zu Archiven, Schränken und Schreibtischen,
- Zutrittskontrollen bei Räumen und Gebäuden mittels Überwachungspersonal oder elektronischer Türsicherungen mit Chipkarten und Code-Tastaturen,
- kontrollierte Weitergabe von Schriftstücken (typisches Beispiel: die Verwendung speziell gekennzeichneter Umlaufmappen und die direkte Weitergabe von Person zu Person gemäß Verteiler).

Auch die generelle Nutzung von Netzwerken kann der Zugriffskontrolle unterliegen, um die unberechtigte Verwendung von Betriebsmitteln der Datenübertragung auszuschließen.

Management

Befassen wir uns zunächst mit dem Management der Zugriffskontrolle. Offensichtlich ist festzulegen, wer was darf, d. h. wir brauchen Regeln, nach denen ein gewünschter Zugriff auf Zulässigkeit oder Unzulässigkeit überprüft werden kann. Wir betrachten dazu vier Methoden, die „klassifizierten Informationen“, das

Need-To-Know-Prinzip, die Zugriffskontrolllisten und die Zugriffskontrolle mittels Verschlüsselung.

Klassifizierte Informationen

Haben wir unsere Daten mit Attributen wie „vertraulich", „geheim", „streng geheim" klassifiziert und sind unsere Subjekte „ermächtigt" zum Umgang mit „vertraulichen", „geheimen", „streng geheimen" Daten, so wäre eine einfache Entscheidungsregel die folgende: Wer für eine bestimmte Klasse ermächtigt ist, darf alle Daten dieser Klasse und ggf. niedrigerer Klassen *lesen*. Beim *Schreiben* muss es umgekehrt sein: Niemand darf Daten einer Klasse in eine Datei einer niedrigeren Klasse schreiben (sonst würde die Information „herabgestuft"). Schreiben darf man also nur nach „oben".

Compartment, Need-To-Know

Es wäre aber auch denkbar, die Daten nach „Vorstandsinformation", „Kundendaten", „Personaldaten" zu klassifizieren. Zugriff zu einem Datum erhalten dann jeweils Mitglieder des Vorstands, das Projektteam für den Kundenauftrag, die Mitarbeiter der Personalabteilung. Klassen dieser Art bezeichnet man als „Compartments". Im Grunde ist dies die Umsetzung des so genannten „Need-To-Know"-Prinzips: „Kenntnis nur, wenn nötig".

Access Control List

Eine weitere Form von Regeln stellen simple Listen dar, in denen je *Objekt* verzeichnet ist, welches Subjekt welchen Zugriff haben darf. Solche Listen nennt man Zugriffskontrolllisten (Access Control Lists, ACL). Die Auswerteregel lautet: Zugriff zu einem Objekt wird einem Subjekt genau dann gestattet, wenn in der Access Control List des Objektes dieser Zugriff als erlaubt verzeichnet ist. Man kann auch genau umgekehrt vorgehen und jedem *Subjekt* alle Objekte zuordnen, für die das Subjekt Zugriffsrechte besitzt. Noch einen Schritt weiter: Man nutzt nicht mehr Listen sondern eine Tabelle bzw. eine Matrix, in der Subjekte / Objekte in der ersten Spalte / Zeile angeordnet sind; im Kreuzungspunkt sind dann die Zugriffsrechte eingetragen: Man spricht von der *Zugriffskontrollmatrix*.

Verschlüsselung

Eine weitere Methode besteht darin, Dateien zu verschlüsseln, und den zugehörigen Schlüssel nur den Befugten „auszuhändigen". Soll eine Datei bearbeitet werden, wird sie vorher entschlüsselt und nach erfolgter Bearbeitung wieder verschlüsselt. Dieses Verfahren ist auch dort anwendbar, wo keine zuverlässige Zugriffskontrolle vorhanden ist – etwa bei der Übertragung in öffentlichen Netzen. Andererseits gibt uns die Methode der Verschlüsselung einige neue Probleme auf, die wir näher im Abschnitt 11.5 behandeln. Bei der Verschlüsselung tritt an die Stelle der Vertraulichkeit der Informationen die Vertraulichkeit des

Schlüssels und ggf. der verwendeten Verschlüsselungsverfahren. Wie man leicht erkennt, lässt sich auf dieser Basis eine *dezentrale* Zugriffskontrolle realisieren.

Berechtigungskonzept

Allen Formen der Zugriffskontrolle ist gemein, dass die Berechtigungen festgelegt und gepflegt werden müssen. Wer nimmt diese Management-Aufgabe wahr? Es gibt dazu zwei Grundkonzepte:

- Der jeweilige „Eigentümer" eines Objektes erlässt solche Regeln für dieses Objekt. Diese Form wird als „benutzerbestimmbare Zugriffskontrolle" bezeichnet.
- Die Regeln werden zentral festgelegt. Hier spricht man von einer „vorgeschriebenen Zugriffskontrolle".

Es ist leicht einsehbar, dass auch Mischformen vorkommen können, bei denen bspw. in einem Unternehmen abteilungsübergreifend eine vorgeschriebene Zugriffskontrolle eingerichtet wird, zusätzlich innerhalb jeder Abteilung benutzerbestimmt Rechte an Objekten der Abteilung vergeben werden können.

Man erkennt, dass das Management der Zugriffskontrolle durchaus komplex sein kein. In solchen Fällen schaltet man ein so genanntes *Berechtigungskonzept* vor, das ggf. eine lokale und globale Rechtevergabe, eine zentrale oder dezentrale Zugriffskontrolle, eine DAC und / oder MAC vorsieht.

Management

Um das Management der Zugriffskontrolle in den Griff zu bekommen, sind folgende Fragen zu beantworten:

- Nach welchem Berechtigungskonzept werden Regeln erlassen?
- Welche Rollen dürfen Regeln erlassen, ändern, löschen?
- Welche Subjekte sind der Zugriffskontrolle zu unterziehen? Gibt es Ausnahmen? Gibt es eine automatische Vererbung von Rechten[44]?
- Für welche Objekte (z. B. Daten, Systeme, Sicherheitsbereiche) sind Regeln anzuwenden? Gibt es Default-Regeln[45]?

---

[44] Erbt z. B. ein von einem Subjekt gestarteter Prozess die Rechte des Subjekts?

[45] Bei Unix wird z. B. durch eine benutzerspezifische Maske gesteuert, welche Rechte der Eigentümer, seine Gruppe und der Rest der Welt an neuen Dateiobjekten erhalten.

– Kann es sich widersprechende Regeln geben und wie werden diese ggf. behandelt?

– Sind bei mehreren anzuwendenden Regeln Reihenfolge-Probleme zu beachten?

Sind mehrere Regeln anzuwenden, hängt die Entscheidung oft von der Reihenfolge des Auswertens der Regeln ab. Typische Beispiele sind hier die Anwendung von Firewall-Regeln, aber auch die Anwendung von SPAM-Filtern in Mailsystemen.

– Wie werden sich überlappende Regeln behandelt?

Hat ein Benutzer Rechte, die an seine User-ID gebunden sind, darüber hinaus aber noch Rechte aus Gruppenzugehörigkeiten, stellt sich die Frage, ob alle Rechte einfach additiv zusammengeführt werden (was der Normalfall ist).

– Zu welchem Zeitpunkt erfolgt eine Zugriffskontrolle?

Zu diesem Punkt einige Anmerkungen und Fragen. Betriebssysteme wickeln den Dateizugriff eines Prozesses meist wie folgt ab: Der Prozess fordert das Öffnen einer Datei an und gibt dabei vielfach an, dass er sie später zu lesen oder / und zu beschreiben gedenkt. Erfasst die Zugriffskontrolle nur das Öffnen einer Datei, aber nicht mehr die eigentlichen Lese- oder Schreibzugriffe? Wird bereits beim Öffnen die Zugriffskontrolle ausgeführt oder erst beim tatsächlichen Lese- oder Schreibzugriff? Was passiert, wenn während der Bearbeitung das Zugriffsrecht durch den System-Administrator entzogen wird? Wird dies sofort wirksam – könnte inkonsistente Dateien nach sich ziehen – oder erst beim nächsten Versuch des Öffnens?

– Welche Maßnahmen werden bei nicht zulässigen Zugriffsversuchen getroffen?

– Wie steht es mit der Vertraulichkeit, Verfügbarkeit und Integrität der Entscheidungsdaten (z. B. die gespeicherten Regeln, die Daten in den Access Control Lists oder in der Zugriffskontrollmatrix)?

In allen (IV-, IT-) Systemen mit vielen Subjekten und Objekten kann vor allem die *Nicht-Überschaubarkeit* der Rechtebeziehungen eine Bedrohung sein. In Folge der Komplexität könnten unbeabsichtigt Regeln eingerichtet oder geändert werden, durch die autorisierten Subjekten der Zugriff verweigert oder nicht-autorisierten Subjekten der Zugriff ermöglicht wird. Kann sich beispielsweise der System-Administrator eines Systems selbst aussperren?

Ein besonderes Problem sind *verdeckte* Rechteänderungen. Sie entstehen meist in folgender Situationen: Ein Subjekt A erhält zur Vereinfachung der Administration dadurch Rechte, dass er einem anderen Subjekt B gleichgesetzt wird (Security Equivalences). Werden für B nun später Rechte geändert, so stellt sich die Frage, ob dann A automatisch betroffen ist. Dies kann erwünscht sein, aber auch ungewollt sein.

Ein Blockade-Problem besonderer Art stellen *nicht mehr änderbare* Rechtebeziehungen dar. Ein bekanntes Netzwerk-Betriebssystem erlaubte in einer älteren Version die Vergabe von Execute-Only-Attributen an Programmdateien. Da diese Dateien nur ausgeführt werden durften, war auch das Ändern der Rechtbeziehungen nicht mehr möglich. Insbesondere konnte einer solchen Datei das Execute-Only-Attribut nicht mehr entzogen, die Datei also nicht mehr gelöscht werden! Gehörte eine solche Datei zu einer Standardsoftware, konnte es sogar Probleme mit dem Einspielen neuer Versionen geben, da die alte Version nicht mehr überschrieben werden konnte – letzte Möglichkeit: Neu-Installation des Systems.

11.4 Wiederaufbereitung

In diesem Abschnitt geht es um so genannte „wiederverwendbare" Speicher: Dazu zählen wir jede Art von Speicher, der ganz oder teilweise „gelöscht" werden kann, um Platz für neue Daten zu schaffen. Zu dieser Gruppe von Speichern zählen Arbeitsspeicher, temporäre Puffer (z. B. in einer Tastatur oder auch der Bildschirm-Speicher, Auslagerungsdateien), Datenträgern wie Disketten, CD-RW und DVD-RW, Festplatten, USB-Sticks usw.

Wiederaufbereitung

Diese Speicher können Daten aus früheren Nutzungen enthalten und müssen deshalb aufbereitet werden, bevor sie erneut zur Nutzung freigegeben werden. Diese Funktion nennt man Wiederaufbereitung (*Object Reuse*).

Die Bedrohungen liegen auf der Hand: Ohne Wiederaufbereitung können vertrauliche Informationen an Unbefugte gelangen.

Als mögliches Verfahren kommt zunächst das Löschen der Daten auf einem Speicher in Frage. Bedenken Sie dabei folgendes: Das Löschen von Dateien mittels Betriebssystem löscht in aller Regel nur die Dateinamen im Verzeichnis, die Daten sind jedoch weiterhin verfügbar und lassen sich oft rekonstruieren. Gelöscht in unserem Sinne werden Daten nur durch Überschreiben. Physikalisch bedeutet dies in aller Regel aber nur eine Reduktion des Signalpegels der alten Daten auf dem Speicher. Mit geeigneten

Werkzeugen lassen sich die überschriebenen Signale oft wieder reproduzieren – insbesondere dann, wenn das Muster der Überschreibung bekannt ist. Jedes Überschreiben reduziert den Signalpegel der ursprünglichen Daten nur um einen bestimmten Betrag.

Fazit: Löschen durch Überschreiben macht bei hohen Sicherheitsanforderungen nur dann Sinn, wenn mehrfach überschrieben wird. Als Faustregel hat sich 7-maliges Überschreiben mit jeweils zufälligen Mustern als ausreichend erwiesen. Das mehrfache Überschreiben ist für viele Rechner allerdings ein Performance-Problem: Schließlich müssen nicht nur gelöschte Nutzerdateien, sondern auch alle zu löschenden System-Dateien einschließlich aller temporären Speicher in gleicher Weise behandelt werden. Ist ein hohes Maß an Vertraulichkeit gefordert, *muss diese Option eingeschaltet* werden.

Nicht überall vorhanden, aber sehr sinnvoll sind spezielle Löschgeräte ("Bulk Eraser") für magnetische Datenträger wie Disketten und Bänder.

Eine andere Methode für „object reuse“ ist, das Lesen des Speichers per Betriebssystem zu verhindern, bevor nicht neue Daten geschrieben worden sind. Dies macht natürlich nur dann Sinn, wenn das Mitnehmen bzw. Entwenden des Datenträgers und Einbau in ein anderes (ungeschütztes) System ausgeschlossen werden kann.

Management

Die Schlüsselfragen zur Wiederaufbereitung lauten:

- Welche Speicher müssen wiederaufbereitet werden?
- Welche Speicher werden nicht wiederaufbereitet, sondern stattdessen (sicher) vernichtet oder (sicher) endgelagert?
- Nach bzw. vor welchen Aktionen muss eine Wiederaufbereitung erfolgen?
- Durch welches technische Verfahren soll die Wiederaufbereitung erfolgen?

11.5 Verschlüsselung

Das vorliegende Buch will keine systematische Einführung in die *Kryptografie* leisten. Vielmehr wollen wir uns darauf beschränken, einige Informationen zusammenzustellen, die zum Grundwissen eines IT-Sicherheitsbeauftragten gehören. Dies betrifft im Wesentlichen

- die Unterteilung in symmetrische und asymmetrische Verfahren,
- das Problem des Schlüsselmanagements (Generierung, Verteilung, sichere Aufbewahrung, Wechsel),
- die Sicherheit der technischen Verschlüsselungskomponente (Hardware / Software).

Krypto-Management

Mit der Verschlüsselung kann man viele Sicherheitsprobleme lösen, sich aber auch neue Probleme einhandeln. Man erkennt vor allem, dass die „Verschlüsselung" eine ganze Reihe von technischen Fragen und Management-Problemen nach sich zieht. In einschlägigen Ratgebern findet man deshalb den Hinweis, ein formelles *Krypto-Management* einzurichten, das sich dieser Probleme annimmt und ggf. sogar ein eigenes Krypto-Konzept erstellt.

Grundlegendes

Algorithmus

In diesem Kontext betrachten wir Daten, die uns in binärer Darstellung vorliegen. Wir führen diese Daten einem mathematischen *Algorithmus* zu und erhalten als Ergebnis die verschlüsselten Daten. Meist sind diese Algorithmen so aufgebaut, dass sie Datenblöcke einer bestimmten Länge verschlüsseln können; man teilt also den Bit-Strom einer Datei in solche Blöcke ein und erhält sukzessive verschlüsselte Datenblöcke, die hintereinander gesetzt die verschlüsselte Datei ergeben.

Padding

Abhängig von Block- und Dateilänge kann es passieren, dass am Ende der Datei nicht mehr ausreichend viele Bits zur Verfügung stehen, um den letzten Block zu füllen: Hierdurch ergibt sich die Notwendigkeit, die Datei mit Dummy-Bits aufzufüllen: Man spricht vom „Padding". Wir beachten hier bereits den Umstand, dass ein Padding ein Sicherheitsproblem darstellen *kann*, wenn neben dem verschlüsselten Wert des letzten Blocks auch viele Bits des Originalblocks bekannt sind. Dies trifft standardmäßig zu, wenn man das Padding etwa durch Auffüllen mit „0" oder einem anderen festen Wert durchführt. Solche „Klar-Geheim-Kompromisse" sind für Code-Knacker immer hoch-interessant. Das Padding wird deshalb meist mit zufälligen Werten ausgeführt.

Als mathematische Algorithmen kommen sinnvollerweise nur solche in Betracht, die umkehrbar sind – andernfalls wäre ein Entschlüsseln nicht möglich. Da man die Art des verwendeten

Algorithmus nicht immer geheim halten kann, wäre es dann allerdings auch Unbefugten möglich, die Umkehroperation – das Entschlüsseln – durchzuführen.

Schlüssel

Aus diesem Grund verwendet man Algorithmen, die von weiteren Parametern – so genannten *Schlüsseln* – abhängen. Erst die Kenntnis der Schlüssel erlaubt die Umkehroperation, das Entschlüsseln der Daten. Der Schlüssel ist folglich unter den Kommunikationspartnern geheim zu halten. Im Grunde hat man das Problem der Vertraulichkeit von Daten durch das Problem der *Vertraulichkeit von Schlüsseln* ersetzt und hofft, dass dieses leichter zu lösen ist.

Schlüssellänge

Eine Methode, einen Algorithmus zu knacken, besteht darin, alle möglichen Schlüssel durchzuprobieren: Schlüssel sind Zahlen bzw. Kombinationen von Bits. Die Anzahl der Bits, die *Schlüssellänge*, bestimmt die Anzahl der Versuche beim Ausprobieren aller Schlüssel und muss deshalb ausreichend groß sein. Geringe Schlüssellängen – wie die z. T. immer noch in Browsern bei bestimmten Algorithmen verwendeten 40 Bit – machen es den Code-Knackern sehr einfach. Man beachte, dass jedes weitere Bit eine Verdopplung der Anzahl auszuprobierender Schlüssel bewirkt. Um vor diesem Hintergrund auf der sicheren Seite zu sein, sollte man heute Schlüssellängen oberhalb von 80 Bit wählen.

Stärke

Die Güte bzw. *Stärke* des verwendeten Algorithmus hängt zunächst von zwei Faktoren ab:

- Von der Schlüssellänge: Je höher die Schlüssellänge, umso mehr Zeit würde benötigt, alle Möglichkeiten durchzuspielen.
- Von der mathematischen Qualität: Es darf insbesondere nicht möglich sein, durch „mathematische Tricks“ die Umkehroperation einfach (z. B. ohne volles Durchprobieren aller Schlüssel) durchführen zu können.

Backdoors

Wenn Letzteres der Fall ist und solche „Tricks“ der Allgemeinheit nicht, den Entwicklern des Algorithmus jedoch sehr wohl bekannt sind, haben wir ein Problem. Man spricht in diesem Zusammenhang von „Hintertüren“ oder „Backdoors“. Es gibt eine Reihe von bekannten Algorithmen, die solche Backdoors beinhalten oder bei denen man zumindest Entsprechendes vermutet. Diese Problematik führt zu der Erkenntnis, nur solche Algorithmen zu verwenden, die öffentlich bekannt und hinreichend untersucht worden sind, um Backdoors möglichst auszuschließen.

Schlüssel-Wechsel

Eine weitere „Hilfe“ für Code-Knacker können umfangreiche Datenmengen sein, die mit dem *gleichen* Schlüssel verschlüsselt worden sind. Schlüssel könnten außerdem im Laufe der Zeit kompromittiert sein, d. h. Unbefugten zur Kenntnis gelangt sein. Aus solchen Überlegungen heraus wird die Forderung abgeleitet, Schlüssel regelmäßig zu wechseln, d. h. durch neu erzeugte zu ersetzen.

Schlüsselgenerierung

Dabei müssen neue Schlüssel so erzeugt werden, dass es keine Gesetzmäßigkeit gibt, mit der aus dem alten Schlüssel auf den neuen Schlüssel geschlossen werden kann, d. h. die Schlüssel müssen „zufällig“ erzeugt werden. Die Schlüsselgenerierung selbst muss natürlich so ablaufen, dass nicht schon hier Unbefugte Kenntnis der Schlüssel erhalten.

Bei manchen Algorithmen kann es vorkommen, dass nicht alle Schlüssel gleichermaßen „gut“ sind: Es kann Zahlenbereiche geben, die man bei der Auswahl von Schlüsseln meiden sollte. Solche Informationen sind einschlägigen Kryptografie-Büchern zu entnehmen.

Schlüsselverteilung

Da die Kommunikationspartner über zu einander passende Schlüssel verfügen müssen, stellt sich im Ablauf zusätzlich das Problem der *Verteilung* der Schlüssel an die Partner. Dabei dürfen Schlüssel nicht so übertragen werden, dass sie abhörbar sind und den Daten, auf die sie sich beziehen, zugeordnet werden können. Aus diesem Grund benötigt man einen in diesem Sinne „sicheren Kanal“ zur Schlüsselübertragung bzw. Schlüsselverteilung. Als Beispiel sei die persönliche Übergabe von Schlüsseln bzw. von Schlüssel-Medien an die Partner genannt oder die elektronische Übertragung auf einem anderweitig gesicherten Netzwerk.

Fassen wir soweit zusammen: Die Sicherheitsmaßnahme „Verschlüsselung“ zur Wahrung der Vertraulichkeit ist in ihrer Wirksamkeit von der Güte der Schlüssel (Länge, Auswahl), der Stärke des Algorithmus und der Sicherheit der Schlüsselgenerierung und Schlüsselverteilung abhängig. Zusätzlich sollten Schlüssel häufig gewechselt werden.

Kryptoeinheit

In der Praxis werden Ver- und Entschlüsselung durch entsprechende Software und / oder Hardware geleistet, im Folgenden als *Kryptoeinheit* bezeichnet. Diese verfügen meist auch über Einrichtungen, „gute“ Schlüssel zu erzeugen. Um zufällige Schlüssel zu erzeugen, verwendet man physikalische Rauschquellen. Die Qualität eines solchen „Zufallszahlengenerators“ ist ein wichtiger Bewertungsfaktor. Welche Attacken auf Kryptoein-

heiten sind denkbar? Unbefugte könnten versuchen, eine Kryptoeinheit zu beeinflussen, indem sie z. B.

- unbemerkt bestimmte Schlüssel einstellen,
- eingestellte Schlüssel auslesen,
- den Algorithmus oder den Schlüssel-Generator manipulieren,
- unverschlüsselte Daten an der Kryptoeinheit vorbeileiten, indem sie Ein- und Ausgang der Kryptoeinheit (logisch oder physisch) „kurzschließen".

Ein anderer „Angriff" besteht darin, Kryptoeinheiten unentdeckt komplett gegen solche auszutauschen, deren Funktion man „beherrscht". Teilweise können die aufgezählten Angriffe „aus der Ferne" durchgeführt werden, wenn Kryptoeinheiten in einem Netzwerk integriert sind, teilweise erfordern sie einen physischen Zugang zu den Kryptoeinheiten. Der Angriff aus der Ferne ist natürlich dann besonders Erfolg versprechend, wenn die Kryptoeinheit durch Software auf einem PC mit Anschluss an das Internet realisiert ist.

Solche möglichen Attacken beim Einsatz von Verschlüsselung müssen wir mit entsprechenden Sicherheitsmaßnahmen abfangen. Insbesondere muss verhindert werden, dass *Unbefugte* Zugriff auf Kryptoeinheiten erhalten, zumindest muss ein Zugriff schnell entdeckbar sein. Andererseits muss man einen *befugten* Zugriff einrichten, um z. B. die Aufgaben des Krypto-Managements ausführen zu können.

Verschlüsselung kann auch dazu genutzt werden, Daten in IT-Systemen „sicher" zu *speichern*, d. h. Unbefugten keinen Lesezugriff zu ermöglichen. Vor der Bearbeitung von Daten sind diese zu entschlüsseln und nach erfolgter Bearbeitung wieder zu verschlüsseln. In diesem Szenario stellt sich allerdings die Frage, ob es Unbefugten möglich ist, die temporär entschlüsselten Daten abzugreifen. Man erkennt, dass man nun den Workflow bei der Bearbeitung systemtechnisch absichern muss, andernfalls könnte man sich den Einsatz der Verschlüsselung sparen.

Schlüssel-Backup

Ein weiteres Problem ergibt sich, wenn Daten entschlüsselt werden sollen und der erforderliche Schlüssel nicht „aufbewahrt" wurde. Bei einem guten Verschlüsselungsverfahren wären dann die Daten verloren (Verlust der Verfügbarkeit), weil es keine Möglichkeit gibt, den richtigen Schlüssel anderweitig zu ermit-

teln. Ein Problem der geschilderten Art könnte sich beispielsweise bei der Ver- und Entschlüsselung von Backup-Tapes ergeben. Dies führt zu der Anforderung, Schlüssel geeignet aufzubewahren (*Schlüssel-Backup*), wobei „geeignet" sowohl „vertraulich" (unzugänglich für Unbefugte), „integer" (ungeändert) und im Bedarfsfall „verfügbar" meint.

Management

Beim vorgesehenen Einsatz von Verschlüsselung sind somit folgende Fragen zu stellen:

- Ist der vorgesehene (mathematische) Algorithmus ausreichend stark?
- Werden Schlüssel ausreichender Länge verwendet?
- Werden zulässige Schlüssel generiert und verwendet?
- Ist das Verfahren der Schlüsselgenerierung sicher?
- In welchen Abständen sind Schlüssel zu wechseln?
- Wie wird die Vertraulichkeit der Schlüssel (bei der Erzeugung, Speicherung und Verteilung) gesichert?
- Wie ist vorzugehen, wenn Schlüssel kompromittiert werden, d. h. Unbefugten zur Kenntnis gelangt sind?
- Wie wird der „Schlüsselverlust" vermieden?
- Wie kann erreicht werden, dass zur Bearbeitung temporär entschlüsselte Dateien *während der Bearbeitung* sicher vor dem Zugriff Unbefugter sind?
- Wie wird die Kryptoeinheit vor Attacken geschützt?

Im Folgenden behandeln wir zwei grundlegende Ansätze zur Verschlüsselung – symmetrische und asymmetrische Verfahren.

Symmetrische Verfahren

Symmetrische Verschlüsselungsverfahren funktionieren so, dass die Algorithmen zum Ver- und Entschlüsseln identisch sind und zum Ver- und Entschlüsseln der gleiche Schlüssel verwendet wird: Wendet man den Algorithmus A mit dem Schlüssel K auf die Daten D an, so erhält man die verschlüsselten Daten V; der Kommunikationspartner wendet denselben Algorithmus A und Schlüssel K auf V an und erhält D (Abbildung 20).

In der Praxis hat dies zur Folge, dass es für die Kryptoeinheit, die den Algorithmus technisch realisiert, keine Rolle spielt, ob ver- oder entschlüsselt werden soll – es wird stets die gleiche Operation ausgeführt.

Typische Beispiele für symmetrische Verfahren sind der

- Data Encryption Standard (DES) mit einer Schlüssellänge von 56 Bit,
- Triple-DES (DES³) mit Schlüssellängen von 112 oder 168 Bit,
- IDEA (Schlüssellänge 128 Bit),
- Advanced Encryption Standard (AES) mit Schlüssellängen von 128, 192 oder 256 Bit.

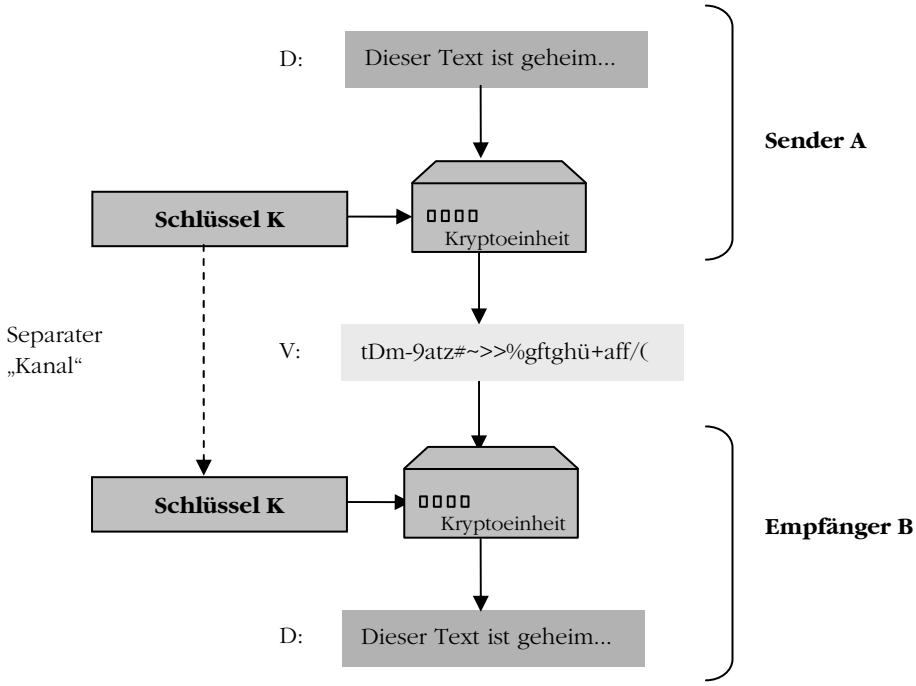

Abbildung 20: Symmetrische Krypto-Verfahren

Wir wollen die dahinter stehende Mathematik nicht weiter behandeln, sondern lediglich festhalten, dass nach gegenwärtiger Erkenntnis Verfahren mit Schlüssellängen *unter 80 Bit nicht mehr verwendet* werden sollen. Damit sind Verfahren wie der DES oder gar RC4/40 Bit abzulehnen.

Performance

Trotz einer gewissen mathematischen Komplexität dieser Verfahren ist man heute in der Lage, mit symmetrischen Verfahren sehr hohe Durchsatzraten zu erzielen, d. h. Performance-Probleme gibt es in aller Regel nicht. Für extrem hohe Raten sind vor allem Hardware-basierte Lösungen geeignet.

In größeren Netzen stellt sich das Problem, ausreichend viele Schlüssel zu generieren, um alle möglichen Kommunikationsbeziehungen abdecken zu können: Sind im Netzwerk n Teilnehmer vorhanden, so benötigen wir für jedes *Paar* von Teilnehmern *einen* Schlüssel, das sind insgesamt n*(n-1)/2 Schlüssel, d. h. die Anzahl benötigter Schlüssel steigt mit dem Quadrat der Anzahl der Teilnehmer, was bei entsprechend großem n ein Problem darstellt – zumal man Schlüssel häufig wechseln möchte.

Asymmetrische Verfahren

Bei asymmetrischen Verschlüsselungsverfahren besitzt jeder Kommunikationspartner *zwei* unterschiedliche Schlüssel (ein Schlüsselpaar) – einen zum Verschlüsseln, einen zweiten zum Entschlüsseln von Daten. Der zum Verschlüsseln vorgesehene Schlüssel wird als „öffentlicher Schlüssel" (*Public Key*) bezeichnet und kann mit dem Namen seines Besitzers z. B.

- in ein öffentlich zugängliches Verzeichnis (*Public Key Directory*) eingestellt werden oder
- an potenzielle Kommunikationspartner auf anderem Wege (z. B. per Email) gesandt werden.

Mit diesem Public Key kann jeder Daten verschlüsseln – aber nur der Besitzer des dazu passenden zweiten Schlüssels ist in der Lage, die Daten zu entschlüsseln. Der zweite Schlüssel wird „geheimer Schlüssel" (*Private Key*) genannt und ist vom Besitzer sicher aufzubewahren.

Als Algorithmus kommt neben anderen das RSA-Verfahren zum Einsatz. Dabei sind die Schlüssellängen je nach Zweck des Einsatzes skalierbar. Dabei sind heute Schlüssellängen von 1024 Bit und höher im Gebrauch. Die hier zugrunde liegende Mathematik ergibt, dass bei vernünftiger Schlüsselauswahl aus dem öffentlichen Schlüssel der dazu gehörende geheime Schlüssel praktisch nicht berechnet werden kann.

Die Abbildung 21 zeigt den Ablauf beim Ver- und Entschlüsseln, wenn Kommunikationspartner A einen Text an B senden möchte. A nimmt den Public Key von B aus einem Directory oder hat ihn vorab zugesandt bekommen. Bei der Übertragung des Public Key sind keine besonderen Sicherheitsauflagen einzuhalten – würde der Schlüssel unterwegs geändert, würde das Verfahren nicht funktionieren, eine Kompromittierung des Private Keys von B ist aber ausgeschlossen.

Der Vorteil asymmetrischer Verfahren ist zunächst die unkomplizierte „Verteilung“ der Public Keys. Zudem ist die Anzahl benötigter Schlüsselpaare genau so groß wie die Anzahl der Kommunikationsteilnehmer, d. h. die Anzahl zu erzeugender Schlüsselpaare steigt linear mit der Anzahl der Kommunikationsteilnehmer.

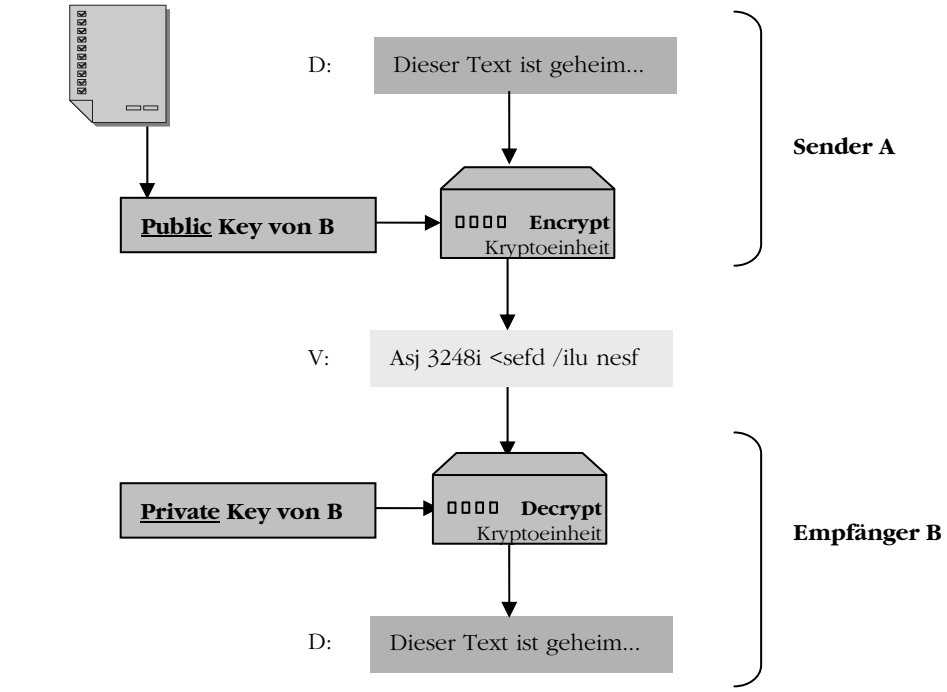

Abbildung 21: Asymmetrische Krypto-Verfahren

Performance

Als Nachteil ist jedoch festzuhalten, dass diese Verfahren wegen ihrer mathematischen Komplexität für die Verschlüsselung von größeren Datenmengen eher ungeeignet sind: Die Performance kann mit den symmetrischen Verfahren bei Weitem nicht mithalten.

Hybrid-Verfahren

Mit einer Kombination von symmetrischen und asymmetrischen Verfahren kann man die Vorteile beider Verfahren kombinieren und ihre Nachteile weitgehend vermeiden. Im Grund funktionieren solche Hybrid-Verfahren so, dass die asymmetrischen Schlüs-

selpaare der Teilnehmer dazu verwendet werden, Schlüssel für symmetrische Verfahren sicher zu übertragen, um dann im zweiten Schritt damit Nutzdaten symmetrisch zu verschlüsseln. Denkt man an die vergleichsweise geringen Schlüssellängen symmetrischer Verfahren, wird klar, dass es bei deren Verschlüsselung mit asymmetrischen Verfahren praktisch kein Performance-Problem geben wird. Wie sieht nun der Ablauf im Detail aus?

Die Kommunikationspartner seien A und B. A verfüge über den Public Key von B. Dann erzeugt A einen Schlüssel K für das später anzuwendende symmetrische Verfahren, verschlüsselt diesen mit dem Public Key von B und überträgt das Ergebnis an B. Teilnehmer B kann mit seinem Private Key den Schlüssel K entschlüsseln und stellt ihn anschließend seiner symmetrischen Kryptoeinheit zur Verfügung.

A hat den Schlüssel K ebenfalls seiner symmetrischen Kryptoeinheit übergeben und beginnt nun damit, die Nutzdaten zu verschlüsseln. Da B über den gleichen Schlüssel K verfügt, kann er die Daten entschlüsseln.

Auf diese Weise hat man die hohe Geschwindigkeit symmetrischer Verfahren mit der einfachen „Schlüsselverteilung“ asymmetrischer Verfahren kombiniert.

Man-in-the Middle

Das geschilderte Verfahren hat allerdings ein grundsätzliches Problem: Der Public Key von B gelangt über das Directory oder auf anderem Wege zu A. Wie kann A sicher sein, dass der erhaltene Public Key wirklich zu B gehört bzw. von B kommt? Es lässt sich zeigen, dass ein so genannter „man-in-the-middle“-Angriff möglich ist, bei dem sich ein Dritter unbemerkt in die Kommunikation einschaltet, sich gegenüber A für B und gegenüber B für A ausgibt und alle übertragenen Daten mitlesen kann.

Letztlich sind solche Attacken nur dann entdeckbar und vermeidbar, wenn die Kommunikationspartner sich gegenseitig „authentisieren“ können, d. h. ihre Identität zweifelsfrei nachweisen können. Um dies zu erreichen, bedient man sich „elektronischer Zertifikate“, die für Personen, Firmen oder auch Rechner (Server und Client) ausgestellt werden (s. Abschnitt „11.7 Elektronische Signatur“).

SSL-Protokoll

Die skizzierten Techniken – Nutzung des Hybrid-Schemas in Verbindung mit Zertifikaten – werden im Rahmen des SSL-Protokolls verwendet, das als „sicheres Protokoll“ für viele Internet-Anwendungen herangezogen wird. Seine reale Sicherheit hängt

allerdings in der Praxis von vielen Parametern ab, für deren Behandlung auf Spezialliteratur[46] verwiesen wird. Im Zusammenhang mit der elektronischen Übermittlung von Konto- und Kreditkartendaten im Internet (z. B. bei Bestellungen in Online-Shops) empfehlen verschiedene Initiativen, SSL nur in Verbindung mit symmetrischen Verfahren ausreichender Schlüssellänge (128 Bit oder höher) zu verwenden.

11.6 Wahrung der Integrität

In den Abschnitten über Grundstrukturen war die Integrität von Daten als eines der grundlegenden Sicherheitsziele erkannt worden. Zur Erreichung dieses Ziels sind Sicherheitsfunktionen erforderlich, die in Sicherheitsstandards häufig als „Unverfälschtheit" oder „Wahrung der Integrität" (Englisch: accuracy) bezeichnet werden. Die Integrität von Daten ist dadurch bedroht, dass

- *Unbefugte* (und ihre Prozesse) unzulässige Änderungen an den Daten vornehmen,
- *Befugte* unbeabsichtigt (Bedienungsfehler, Fahrlässigkeit) oder beabsichtigt unzulässige Änderungen durchführen,
- ungewollte Änderungen durch technische *Defekte* oder *Störungen* verursacht werden.

In aller Regel kommt der Zugriffskontrolle die Aufgabe zu, *Unbefugten* das Ändern von Daten und Relationen zwischen Daten in einem IT-System zu verwehren. Ganz anders liegt der Fall in Netzwerken, bei denen eine zentrale Zugriffskontrolle meist nicht realisiert werden kann und organisatorische Maßnahmen nicht greifen. Eine zugriffsgeschützte Leitungsführung wird man nur in seltenen Fällen einrichten können. Mit anderen Worten: Insbesondere in „offenen" Netzwerken haben wir ein Problem…

Data Integrity

Vielfach definiert man die Integrität bei der Übertragung in Netzwerken so, dass die „relevanten" Daten an allen dazu erforderlichen Stellen zweifelsfrei aus dem Datenstrom rekonstruierbar sein müssen. Relevant sind die Nutzdaten und die Verbindungsdaten (Sender, Empfänger). Es soll nicht möglich sein, Adress- und Nutzdaten verändern zu können.

Es bleibt die Frage, wie man das Problem der Datenänderung durch *Befugte* behandelt. Hier helfen meist nur organisatorische Maßnahmen (z. B. Vier-Augen-Prinzip bei der Bearbeitung von

[46] als Einstieg: http://de.wikipedia.org/wiki/Secure_Sockets_Layer

Daten, unabhängige Plausibilitätskontrollen) im Umfeld der IT-Systeme. Technische *Defekte* und *Störungen* kann man nicht gänzlich vermeiden. Hier wäre es schon gut, wenn man solche Vorkommnisse sicher entdecken könnte…

Man gibt sich generell oft damit zufrieden, unzulässige Änderungen *entdecken* zu können. Hierfür gibt es eine ganze Reihe von Verfahren:

– Prüfsummen

Hier werden vorher festgelegte Pakete von Daten aufsummiert und die Summen den Datenpaketen hinzugefügt. Bei Bedarf kann die Summe erneut berechnet und mit dem gespeicherten Wert verglichen werden. Bei Abweichungen haben wir einen Integritätsverlust. Stimmen die Werte jedoch überein, ist keine Garantie für die Integrität der Daten gegeben, da übereinstimmende Summen bei sehr vielen Kombinationen von Daten entstehen können.

– Fehlerkorrigierende Codes

Mit solchen „Codierungen“ von Daten können einzelne Bitfehler sicher entdeckt werden – mehr noch, man erhält eine Information, welchen Wert das defekte Bit ursprünglich besaß. Auf diese Weise lässt sich eine endliche Anzahl von Bitfehlern in Datenpaketen sicher entdecken und beheben; der zu zahlende Preis besteht darin, dass die ursprünglichen Datenpakte durch Hinzufügen der Codierungsinformationen verlängert werden. Solche Verfahren werden in der Praxis verwendet, um z. B. das Kippen von Bits auf Speichern, Bit-Störungen bei Datenübertragungen zu erkennen.

– Hashen von Daten

Hier wird einem Datenpaket ein *Hash-Wert* hinzugefügt; ein solcher Hash-Wert entsteht durch Komprimierung der Daten mittels einer kryptografischen Funktion. Eine solche Kompression ist meist verlustbehaftet, d. h. man kann die ursprünglichen Daten nicht mehr aus dem Hash-Wert zurückrechnen. Gute Hash-Funktionen besitzen aber die Eigenschaft, „kollisionsfrei“ zu sein, d. h. es ist praktisch nicht möglich, zu einem Dokument ein zweites mit gleichem Hash-Wert zu finden. Solche Änderungen wirken sich mit hoher Wahrscheinlichkeit auf den Hash-Wert aus und machen entsprechende Versuche entdeckbar.

– Elektronische Signaturen

Signaturen entstehen dadurch, dass Daten gehasht und anschließend der Hash-Wert mit einem asymmetrischen Kryptoverfahren verschlüsselt wird. Da der dabei zum Einsatz kommende (private) Schlüssel kann einer bestimmten Person zugeordnet sein, so dass die Signatur nicht nur Datenänderungen erkennen lässt, sondern auch noch Auskunft liefert, wer den Datensatz „unterschrieben" hat. Es ist klar, dass Signaturen damit hervorragend für das Versenden von Nachrichten z. B. in Email-Systemen geeignet sind und Änderungen der Daten erkennen lassen. Wir behandeln das Thema „Elektronische Signatur" im nächsten Abschnitt 11.7.

– Einsatz von „Virenschutz-Systemen"

Virenschutz-Systeme stellen eine populäre Maßnahme zur Entdeckung des Verlustes der Integrität von ausführbaren Dateien dar, sind jedoch in ihrer Wirkung beschränkt, da diese u. a. von der Aktualität der Referenzdaten abhängt. Bleiben wir bei diesem Fall und unterstellen, dass wir die ausführbaren Dateien in einem IT-System elektronisch signiert haben. Wird vor jeder Ausführung der Datei die Signatur durch das Betriebssystem nachgerechnet und mit dem registrierten Wert verglichen werden, würden Änderungen mit einer sehr hohen Wahrscheinlichkeit erkannt werden. Wird dieses Verfahren extensiv genutzt, kann es jedoch je nach Leistung des IT-Systems zu Performance-Problemen kommen. Außerdem kann es sein, dass intelligente Viren Programme erst dann infizieren, wenn die Signaturprüfung erfolgt ist und das ausführbare Programm im Arbeitsspeicher des betreffenden IT-Systems steht.

Weiterhin ist die Liste der Referenz-Signaturen extrem sicherheitskritisch. Wichtige Regel deshalb: Eine generelle Signaturprüfung ist nur dann voll wirksam, wenn weder der Prüfvorgang noch die Referenzdaten „beeinflussbar" sind. Dies führt in unserem Beispiel zu der Forderung, dass zumindest das Betriebssystem auf dem betreffenden Rechner einen hohen Integritätsschutz benötigt.

Management

Vor dem Einsatz von integritätswahrenden Maßnahmen ist zu klären,

– für welche Objekte die Integrität besonders gesichert bzw. ein Integritätsverlust entdeckbar sein muss,
– wodurch die Integrität verletzt werden kann,
– welche Verfahren dem entgegen wirken sollen,

– wann eine Verletzung der Integrität bemerkt werden soll,
– welche Maßnahmen bei Entdeckung eines Integritätsverlustes zu ergreifen sind.

11.7 Elektronische Signatur

Grundsätzliches Verfahren

Die elektronische Signatur ist ein Mittel, um

– Daten mit der Identität eines Teilnehmers (einer Person, einer Institution oder eines Rechners) zu verknüpfen und
– nach erfolgter Signatur spätere Änderungen an den Daten erkennen zu können.

Hierzu verwendet man asymmetrische Krypto-Verfahren – allerdings in einem anderen Sinne als bei der Daten-Verschlüsselung:

Teilnehmer A möchte Daten D „signieren", um seine Identität mit D zu verknüpfen und spätere Änderungen an D entdeckbar zu machen. Dazu verschlüsselt A die Daten D mit seinem *Private Key*, die verschlüsselten Daten wollen wir mit V bezeichnen.

Jeder, der nun über den dazu gehörenden *Public Key* von A verfügt – also im Grunde wirklich „jeder" -, kann die Daten V entschlüsseln. Vergleicht man nun D und das entschlüsselte V, würde man Änderungen erkennen können. Zeigt der Vergleich eine Übereinstimmung, ist auch klar, dass die Daten mit dem zuvor genannten *Private Key* von A signiert worden sind: Wären die Daten mit einem anderen (Private) Key verschlüsselt worden, würde der Vergleich zwischen D und V keine Übereinstimmung ergeben.

Für diese Vorgehensweise ist festzuhalten, dass neben den verschlüsselten Daten V auch immer die Originaldaten D mit übertragen werden müssen, andernfalls ist ja der Vergleich nicht möglich. Damit wird auch sofort ein gängiges Missverständnis aufgeklärt: Mit der elektronischen Signatur werden die entsprechenden Daten nicht gegen den Verlust der Vertraulichkeit geschützt, vielmehr können (nur) Verletzungen der Integrität erkannt werden.

Hash

Die asymmetrischen Verfahren sind aus Performance-Gründen für die Verschlüsselung größerer Datenmengen eher nicht geeignet. Deshalb geht man so vor, die zu signierenden Daten zunächst geeignet zu komprimieren („hashen"). Dabei geht natürlich Information verloren. Das Kompressionsverfahren sollte aber

zumindest so beschaffen sein, dass es „kolllisionsfrei“ ist, d. h. es sollte praktisch unmöglich sein, zwei (sinnvolle) Dokumente mit dem gleichen „Hash-Wert“ zu erzeugen. Solche Hash-Verfahren sind u. a. RIPEMD und die SHA-Familie. Sie komprimieren vorgegebene Daten zu einem Hash-Wert fester Länge, z. B. 160 Bit (andere Längen sind möglich).

Für die Signatur verschlüsselt werden nun nicht mehr die gesamten Daten D, sondern nur ihr Hash-Wert H_D, als Ergebnis erhalten wir $V(H_D)$. Der Empfänger von „D plus $V(H_D)$“ erzeugt nun mit demselben Hash-Verfahren aus D einen Hash-Wert H*, entschlüsselt dann $V(H_D)$ mit dem Public Key des Absenders und vergleicht das Resultat mit H*: Stimmen beide Werte überein, hat er die Integrität der Daten verifiziert. Zugleich ist damit klar, dass die Daten vom Teilnehmer A (= Inhaber des Public Keys) signiert wurden.

Wie man erkennt, müssen folgende Daten beim Empfänger vorliegen, um alle Prüfungen durchführen zu können:

- die Originaldaten D,
- der vom Absender ermittelte und signierte Hashwert $V(H_D)$,
- die Information, welches Hash-Verfahren angewendet wurde bzw. anzuwenden ist,
- der Public Key des Absenders,
- die Information, welches asymmetrische Verfahren bei der elektronischen Signatur angewendet wurde.

Elektronische Identität und deren Prüfung

Eine wesentliche Frage ist noch nicht beantwortet: Wie kann der Empfänger verifizieren, dass die erhaltenen Daten tatsächlich von dem vermuteten Absender stammen? Im Grunde könnten bei einer geringen Teilnehmerzahl die Teilnehmer selbst eine persönliche Übergabe der Public Keys vorsehen und dabei jeweils gegenseitig eine Identitätsprüfung vornehmen. Dies ist allerdings bei großer Teilnehmerzahl oder bei größeren räumlichen Distanzen nicht praktikabel.

Trust Center

Vor diesem Hintergrund kommt nun ein „vertrauenswürdiger Dritter“ – ein „Trust Center“ – ins Spiel: Es

- prüft einmalig die Identität der Teilnehmer (*Registrierung*),

- generiert auf Wunsch Schlüsselpaare für die Teilnehmer (*Schlüsselgenerierung*)[47],
- stellt „Zertifikate“ über die Zuordnung Identität ↔ Schlüssel(paar) aus (*Zertifizierung*),
- übergibt Zertifikate und ggf. Schlüsselpaare an die Teilnehmer,
- trägt die Zertifikate in die Liste der gültigen Zertifikate ein und gibt Dritten über deren Gültigkeit elektronische Auskünfte (*Verzeichnisdienst*),
- nimmt Sperrungen von Zertifikaten entgegen (*Sperrdienst*) und veröffentlicht unter Umständen regelmäßig „Sperrlisten“.

Wir behandeln die aufgezählten Dienste der Reihe nach und beantworten die eingangs gestellte Frage im Anschluss daran.

Im Folgenden werden wir als Beispiel oft die Verhältnisse beim deutschen Signaturgesetz (/SigG/) heranziehen. Beim SigG werden Trust Center als „Zertifizierungsdiensteanbieter“ (ZDA) bezeichnet, andernorts verwendet man auch die englische Bezeichnung „Certification Service Provider“ (CSP).

Im SigG werden einfache, fortgeschrittene, qualifizierte Signaturen und „qualifizierte Signaturen mit Anbieter-Akkreditierung“ begrifflich unterschieden. Wir wollen hier auf die Unterscheide nicht eingehen. Nur für die letzten beiden Stufen (qualifiziert, qualifiziert und akkreditiert) definiert das SigG Sicherheitsanforderungen und erreicht damit eine sehr hohe Sicherheit. Dies hat zur Folge, dass inzwischen in vielen anderen Gesetzen, die eine Unterschrift von Personen unter Dokumenten verlangen, die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgestellt ist.

Registrierung

In sehr einfach gelagerten Fällen läuft die Registrierung wie folgt ab: Man schickt eine Email mit einigen Daten (im Wesentlichen seine Emailadresse) an ein Trust Center und erhält ebenfalls per Email einen PIN-Code an seine angegebene Emailadresse geschickt. Damit loggt man sich auf einer Web-Site des Trust Centers ein, ruft das Zertifikat und das Schlüsselpaar ab und installiert diese in seinem Browser. Bei diesem Beispiel läuft die Identifikation also nur über die Emailadresse – ein bescheidener Si-

[47] Vielfach kann der Teilnehmer auch von ihm selbst erzeugte Schlüssel vorlegen.

cherheitsgewinn, der keinesfalls ausreicht, um wirklich eine Identität *nachzuweisen*.

Andere Verfahren basieren auf dem persönlichen Erscheinen des Teilnehmers bei der *Registrierungsstelle* des Trust Centers: Hier wird die Identität anhand der Ausweisdokumente überprüft und erst dann der weitere Ablauf initiiert.

PostIdent

In Deutschland wird vielfach das PostIdent-Verfahren angewendet, bei dem die Identifizierung und Ausweisprüfung am Postschalter erfolgt. Das Prüfergebnis wird dann von der Post dem jeweiligen Trust Center geeignet übermittelt. Die Post fungiert hier also als „Registrierungsstelle".

Besitzt der Teilnehmer bereits ein Zertifikat (ausreichender Qualität), kann ein neues Zertifikat auch per Email-Antrag mit elektronischer Signatur erfolgen. Die Registrierung beschränkt sich dann auf die Prüfung der Signatur des Antrags.

SigG

Konform zum deutschen Signaturgesetz sind nur das persönliche Erscheinen bei einer Registrierungsstelle und die Vorlage amtlicher Ausweispapiere (Personalausweis, Reisepass mit Meldebescheinigung) sowie die elektronische Antragstellung mit einem bereits vorhandenen qualifizierten Zertifikat.

Schlüsselgenerierung

Soweit ein Trust Center zu den verwendeten Algorithmen passende Schlüsselpaare für die Teilnehmer generiert, ist festzustellen, dass dieser Vorgang hoch sicherheitskritisch ist. Jede Kompromittierung der Schlüssel ist auszuschließen, andernfalls haben darauf basierende spätere Signaturen keine Beweiskraft mehr. In Verfahren, die zur Schlüsselspeicherung und -anwendung Smartcards verwenden, wird deshalb immer häufiger die Schlüsselgenerierung auf die Smartcard selbst verlagert, so dass man ein in sich geschlossenes System hat.

SigG

Im Rahmen des SigG dürfen nur Algorithmen und Schlüssellängen verwendet werden, die von der zuständigen Bundesnetzagentur (BNetzA) als geeignet anerkannt sind. Hierdurch wird insbesondere erreicht, dass erzeugte Schlüssel einmalig sind. Entsprechende Schlüssel-Generatoren müssen nach den Standards ITSEC oder Common Criteria evaluiert und sicherheitsbestätigt worden sein. Die Nutzung eines solchen Schlüssel-Generators durch ein Trust Center darf nur in ausreichend gesicherten Räumlichkeiten erfolgen, was durch eine unabhängige Prüfung zu bestätigen ist.

Zertifizierung

Beim Vorgang der Zertifizierung stellt das Trust Center ein *Zertifikat* über die Zuordnung Identität ↔ Schlüssel(paar) aus. Dabei kann es sich um Schlüssel handeln, die das Trust Center für

den Teilnehmer erzeugt hat, oder um solche, die vom Teilnehmer selbst erzeugt und vorgelegt worden sind.

Ein elektronisches Zertifikat muss eine Reihe von Daten[48] beinhalten:

- Angaben zur Identität des Teilnehmers,
- der Public Key des Teilnehmers und Angaben über das zugeordnete Kryptoverfahren,
- Angaben zum Hash-Verfahren beim Teilnehmer,
- Angaben zum ausstellenden Trust Center,
- Art des Zertifikats (z. B. „qualifiziertes Zertifikat nach dem deutschen Signaturgesetz"),
- die elektronische Signatur des Trust Centers über die Daten des Zertifikats.

Wesentlich ist die Frage, ob solche Zertifikate nicht gefälscht werden können. Dies wird dadurch verhindert, dass das Trust Center jedes ausgestellte Zertifikat elektronisch signiert: Es verwendet dazu ebenfalls ein asymmetrisches Kryptoverfahren und ein entsprechendes Schlüsselpaar. Der Public Key des Trust Centers wird geeignet veröffentlicht oder von einem vertrauenswürdigen Dritten in einem Verzeichnis vorgehalten: Damit kann jedes vom Trust Center tatsächlich oder vermeintlich ausgestellte Zertifikat auf nachträgliche Änderungen oder falsche Identität geprüft werden. Die Beweiskette hängt natürlich daran, dass der Public Key des Trust Centers auf sicherem Wege zum Anwender gelangt und zweifelsfrei zu diesem Trust Center gehört.

SigG

Legen Teilnehmer selbst erzeugte Schlüssel einem Trust Center zur Zertifizierung vor, so muss sich dieses von der „Qualität" der Schlüssel überzeugen, bevor es sie „zertifiziert".

Beim deutschen Signaturgesetz hat man die Bundesnetzagentur (BNetzA) beauftragt, die so genannte „root" als „Sicherheitsanker" zu etablieren. In dieser Funktion stellt die BNetzA ihrerseits Schlüsselpaare und Zertifikate für Trust Center aus und betreibt einen entsprechenden Verzeichnisdienst. Will man nun das Zertifikat bzw. die elektronische Signatur eines Trust Centers verifizieren, fragt man beim Verzeichnisdienst der root an und enthält entsprechende (signierte) Auskünfte. Als

[48] Der genaue Aufbau und die Inhalte des Datensatzes sind in einschlägigen Standards bzw. RFCs beschrieben, z. B. das bekannte X.509 Format.

letzte Sicherheit muss natürlich der Public Key der BNetzA veröffentlicht sein, was über die Web-Site der BNetzA (www.bundesnetzagentur.de) und durch andere Veröffentlichungen bewerkstelligt wird.

Zertifikats- und Schlüsselübergabe

Zertifikat und ggf. generierte Schlüssel werden dem Teilnehmer übergeben. Insbesondere die Übergabe des Private Keys muss auf sicherem Wege erfolgen, er muss weiterhin „sicher" aufbewahrt werden. Zum Signieren muss der Private Key der Kryptoeinheit des Teilnehmers zugeführt werden. Diese Vorgänge sind allesamt hochkritisch, weil bei jedem Transport der Private Key kompromittiert werden könnte. Man erkennt, dass die sichere Übergabe, Speicherung und Anwendung des Private Keys wesentliche Faktoren für die Sicherheit der elektronischen Signatur darstellen. Die in vielen praktizierten Verfahren übliche Speicherung des Private Keys als Datensatz auf einem PC (der möglicherweise ungeschützt am Internet hängt) kann keine verlässliche Sicherheit bieten.

SigG

Zertifikat und Schlüssel werden auf einer Smartcard gespeichert, die mit einem sicheren Auslieferungsverfahren an den entsprechenden Teilnehmer ausgegeben wird. Erst wenn sichergestellt ist, dass die Karte den rechtmäßigen Inhaber erreicht hat, darf das Trust Center das Zertifikat „scharf" schalten, d. h. Anfragen zu seiner Gültigkeit positiv beantworten oder das Zertifikat in seinen Verzeichnisdienst zum Abruf aufnehmen.

Gesetzeskonforme Smartcards (solche, die evaluiert und sicherheitsbestätigt sind) speichern den Private Key auslesegeschützt und führen die Signatur (Verschlüsselung von Hash-Werten) auf der Karte selbst durch. Der Private Key verlässt die Karte also grundsätzlich nie. Um bei Verlust der Karte zu verhindern, dass der „Finder" nun unter falschem Namen signiert, sind alle Karten nach dem deutschen Signaturgesetz mit einem PIN-Verfahren gesichert, d. h. bevor eine Signatur erzeugt werden kann, muss der Veranlassende den korrekten PIN-Code eingeben. Damit liegt eine Authentisierung durch Besitz (der Karte) und Wissen (PIN) vor. Nach einer festgelegten Zahl von Fehlversuchen bei der PIN-Eingabe wird die Smartcard gesperrt und kann ggf. erst unter Anwendung eines so genannten PUK-Verfahrens wieder entsperrt werden.

Verzeichnisdienst

Um Dritten die vollständige Prüfung von Signaturen einfach zu ermöglichen, betreiben Trust Center einen Verzeichnisdienst: Hiermit werden (elektronische) Anfragen zur Gültigkeit eines Zertifikats beantwortet; die Zertifikate von Teilnehmern können sogar abrufbar vorgehalten werden. Auch solche Auskünfte könnten gefälscht oder anderweitig geändert den Anfragenden erreichen. Um dies entdeckbar zu machen, können Auskünfte vom jeweiligen Trust Center elektronisch signiert werden. Volle

Sicherheit erhält man bei der Prüfung eines elektronischen Zertifikats eines Teilnehmers also durch

- eine Verzeichnis-Anfrage beim ausstellenden Trust Center und
- durch Prüfung des Zertifikats des Trust Centers.

Letzteres erfolgt unter Nutzung des veröffentlichten Public Key der Trust Centers oder durch Prüfung über Verzeichnisdienste, die dieses Zertifikat und seinen Status gespeichert haben.

SigG

Alle Verzeichnis-Auskünfte müssen grundsätzlich mit einer qualifizierten elektronischen Signatur versehen sein. Im Falle der root werden deren Public Keys für Prüfzwecke auf verschiedenen Wegen veröffentlicht. Im Rahmen des SigG nimmt man die Prüfung des Zertifikats des Trust Centers durch eine Verzeichnis-Anfrage bei der root vor. Teilnehmer können im Rahmen des Antragsverfahrens akzeptieren oder ablehnen, dass ihr Zertifikat durch Dritte aus dem Verzeichnis abgerufen werden kann.

Sperrdienst

Will man – aus welchen Gründen auch immer, z. B. bei Verlust der Karte oder bei Beendigung der Geschäftsbeziehung zu einem Trust Center – sein Zertifikat sperren lassen, wendet man sich telefonisch, über das Internet, per Brief oder durch persönliches Erscheinen an den *Sperrdienst* seines Trust Centers, der die Sperrung umgehend durchführt. Die Person, die eine Sperrung beantragt, muss sich gegenüber dem Trust Center entsprechend authentisieren. Um Missbrauch z. B. mit verloren gegangen Karten zu verhindern, muss eine Sperrung jederzeit und „schnell" durchführbar sein.

Sperrliste

Vielfach bieten Trust Center einen Sperrlisten-Dienst an, mit dem in bestimmten Abständen (z. B. einmal täglich) die Liste der bei diesem Trust Center gesperrten Zertifikate an Kunden versandt wird. Hierdurch kann man das Verfahren der Prüfung von Signaturen etwas verkürzen (die Anfrage beim Verzeichnisdienst kann sich erübrigen) – allerdings mit dem Risiko, dass seit dem letzten Empfang der Sperrliste zwischenzeitlich ein Zertifikat gesperrt worden sein könnte.

SigG

Beim SigG werden hohe Anforderungen an die Verfügbarkeit des Verzeichnisdienstes und des Sperrdienstes gestellt. Wird eine Sperrung telefonisch beantragt, muss sich der Antragsteller authentisieren. Dies geschieht z. B. durch ein „Sperrpasswort", das der Teilnehmer im Rahmen der Registrierung ausgewählt hat. Eine Sperrung ist darüber hinaus in schriftlicher Form oder durch eine Email, die qualifiziert elektronisch signiert ist, möglich.

Auch wenn die Übermittlung von Sperrlisten nach SigG zulässig ist, sind nur die online-Verzeichnis-Auskünfte als gesetzlich bindend anzusehen. Sperrlisten werden möglicherweise nur im Intervall von Stunden aktualisiert – es könnte also ein Zertifikat zwischenzeitlich gesperrt worden sein, ohne dass dies in der „alten" Sperrliste erkennbar ist.

Vorgang des Signierens

Verfügt ein Teilnehmer über entsprechende Schlüssel und ein diesbezügliches Zertifikat, kann er diese zum Signieren von „Dokumenten" verwenden. Dazu kommt in der Regel eine Software zur Anwendung, mit der die zu signierende Datei ausgewählt und ggf. nochmal angezeigt wird; anschließend werden der Hash-Wert und schließlich die Signatur berechnet. Die Signatur wird zusammen mit der Datei gespeichert und / oder versandt.

SigG

Vor dem Hintergrund der Beweiskraft einer elektronischen Signatur beim SigG wird dem Nutzer dringend nahe gelegt, eine evaluierte und sicherheitsbestätigte Signaturanwendungskomponente (SAK) einzusetzen. Die SAK steuert die Datei-Auswahl, die sichere Anzeige des Inhalts, hasht die Datei und sendet den Hash-Wert unter Nutzung eines sicheren Kanals an die Smartcard, die ihrerseits die Signatur berechnet und zurückschickt.

Die Smartcard des Nutzers wird durch PIN-Eingabe (in der Regel an der Tastatur des Chipkarten-Lesegeräts) aktiviert. Nach der PIN-Eingabe kann genau eine Signatur erzeugt werden. Will man weitere Signaturen erzeugen, ist jedes Mal eine erneute PIN-Eingabe erforderlich. So genannte „Massen-Signaturen" nach einmaliger PIN-Eingabe sind nur in besonders gesicherten Umgebungen gesetzlich zulässig.

Die SAKs verfügen meist auch über die Funktion, erhaltene signierte Dateien zu verifizieren, d. h. die Integrität zu prüfen und die Zertifikatskette bis zur root überprüfen zu können.

Fassen wir zusammen: Verfahren der „elektronischen Signatur" existieren in unterschiedlicher Qualität und Sicherheit. Beides hängt von den Antworten auf folgende Fragen ab:

- Wodurch wird die Identität eines Trust Centers verifizierbar?
- Welche Sicherheit bieten die vom Trust Center vermittelten Dienste?
- Wodurch weist sich ein Teilnehmer gegenüber einem Trust Center aus?
- Welches mathematische Verfahren wird für die elektronische Signatur genutzt?
- Wer generiert die Schlüsselpaare und nach welchem Verfahren geschieht dies?

- Ist das Schlüsselpaar einmalig (oder kann es auch einem zweiten Teilnehmer zugeordnet worden sein)?
- Wie werden Zertifikat und Schlüsselpaar an den Teilnehmer ausgeliefert?
- Wie wird erreicht, dass der Private Key des Teilnehmers nur von diesem genutzt werden kann?
- Wie sicher ist die Kryptoeinheit[49] des Teilnehmers, mit der die elektronische Signatur erzeugt wird?
- Mit welcher Zuverlässigkeit können Dritte die Unterschrift des Teilnehmers verifizieren?

Letzteres ist in einem doppelten Sinne zu verstehen: Welchen Beweiswert hat eine positive Verifikation einer elektronischen Signatur? Ist sie z. B. rechtlich bindend? „Zuverlässig" meint aber auch, dass es Dritten *jederzeit* möglich sein muss, die Verifikation durchzuführen; dabei handelt es sich also um eine Anforderung an die Verfügbarkeit des Verzeichnisdienstes eines Trust Centers.

Attribute

Diesem Abschnitt lag die Vorstellung zugrunde, dass ein „Teilnehmer" eine natürliche Person ist. Nach *deutschem* Signaturgesetz dürfen qualifizierte Zertifikate nur für *natürliche Personen* ausgestellt werden. In der Praxis kommt es aber häufig vor, dass eine Person stellvertretend für eine Institution unterschreibt und – wenn nötig – die Befugnis zur Unterschrift nachweisen möchte. Mit personengebundenen Zertifikaten kann man dies dadurch realisieren, dass im Zertifikat oder in einem separaten *Attribut-Zertifikat* die Unterschrifts-Vollmacht eingetragen wird. Nach den Signaturgesetzen *anderer Länder* (z. B. der Schweiz) kann ein qualifiziertes Zertifikat aber auch für Institutionen (Firmen, Behörden) ausgestellt werden.

Server-Zertifikate

Schlussendlich begegnet man auch dem Problem, dass sich *Rechner* in einem Netzwerk gegenseitig oder gegenüber Subjekten „ausweisen" möchten. Hier kommen „Maschinen-Zertifikate" oder „Server-Zertifikate" zum Einsatz. Viele Trust Center bieten neben den SigG-konformen Diensten auch die Ausstellung von Server-Zertifikaten an.

---

[49] Hier ist auch die Frage wesentlich, ob eine solche Kryptoeinheit auf einer sicheren Plattform (Rechner, Betriebssystem, Netzwerkanbindung) bzw. in sicherer „Umgebung" betrieben wird.

11.8 Verfügbarkeit von Daten

In den Abschnitten über die Grundstrukturen haben wir das Sicherheitsziel *Verfügbarkeit* und einige Beispiele zu dessen Erreichung kennen gelernt.

Zugriffskontrolle

Mit einer funktionierenden Zugriffskontrolle kann zumindest verhindert werden, dass *Unbefugte* die Verfügbarkeit von Daten manipulativ oder unabsichtlich beeinträchtigen. Geht es um Daten, die außerhalb von IT-Systemen (z. B. in Tresoren, Aktenschränken, etc.) gespeichert sind, gilt sinngemäß das Gleiche: Aus „Zugriffskontrolle“ wird dann die Kontrolle des Zugangs zum Ort der Datenhaltung, die Kontrolle über Schlüssel zum Öffnen von Tresoren usw.

Der missbräuchlichen Vorenthaltung von Daten durch *Befugte* kann man in vielen Fällen mit einer Begrenzung der Betriebsmittel (z. B. verwendeter Speicherplatz, Anzahl laufender Prozesse und deren Prioritäten, Anzahl von aufgebauten Verbindungen, usw.) entgegen wirken. Die Begrenzung der Betriebsmittel kann im Betriebssystem eines Rechners oder in den Applikationen integriert sein.

Redundanz

Um Daten grundsätzlich – in welchen Situationen auch immer, vor allem bei technischen Defekten und Elementarereignissen – verfügbar zu halten, ist die Redundanz der Daten das wesentliche Hilfsmittel. Für die Datenverfügbarkeit heißt das, sich Kopien der Daten (*Backup*) anzulegen, auf die im Bedarfsfall zurückgegriffen werden kann.

Management-1

Dabei sind folgende Fragen zu stellen:

- Welche Daten sind zu sichern?
- Wann und in welchen Abständen sind Backups zu erzeugen?
- Welche Medien kommen für das Backup in Frage?
- Wie lange dauert die Bereitstellung der Daten vom Backup?
- Ist die Aktualität der bereitgestellten Daten gegeben bzw. wie viel Verlust ist zu erwarten?

Betrachten wir zwei Beispiele:

- Plattenspiegelung

Hier werden Daten bei der Speicherung parallel auf *mehrere* Platten geschrieben und sind damit bei Ausfall einer Platte (gleich welcher Ursache) nach wie vor verfügbar. Steuert man die Platten noch über unabhängige Controller an, um das Pro-

blem des Controller-Ausfalls abzudecken, kann man einen hohen Grad an Datenverfügbarkeit erreichen. Diese Überlegungen führen zu den bekannten RAID-Systemen. Charakteristiken dieses Verfahrens sind also: *Alle* Daten einer Platte werden gesichert, Kopien werden permanent (ohne Zeitverzug) geschrieben, die Bereitstellung der Daten im Fall der Fälle erfolgt meist verzögerungsfrei. Ein echter Datenverlust ist extrem unwahrscheinlich (abhängig von der Anzahl gespiegelter Platten).

– Auslagerung auf ein separates Medium

Typischer Fall hierfür ist die Auslagerung auf ein Backup-Tape oder ein optisches Speichermedium. Hierbei wird konzeptionell festgelegt, wann bzw. in welchen Abständen ein Backup zu erfolgen hat, welche Daten dabei zu sichern sind und wie ggf. eine bestimmte Anzahl von Medien zyklisch verwendet werden soll. Die Bereitstellung der Daten vom Backup (*Restore*) kann unter Umständen eine erhebliche Zeit in Anspruch nehmen. Dabei wird es immer wieder vorkommen, dass die bereitgestellten Daten einen älteren Stand haben, da seit dem letzten Backup eine bestimmte Zeitspanne vergangen ist, in denen Daten geändert, gelöscht oder hinzugefügt worden sind.

Charakteristiken dieses Verfahrens sind also: zu sichernde Daten auswählbar, Zeitpunkt und Frequenz auswählbar, Bereitstellung zeitaufwändig, Datenaktualität problematisch.

Ein oft vernachlässigtes Thema beim zweiten Beispiel ist die Aufbewahrung der Sicherungsmedien. Erstellt man Backups, um etwa nach einem Brandfall oder anderen Elementarereignissen auf die Daten zurückgreifen zu können, macht es wenig Sinn, die Medien an dem gleichen Ort zu lagern wie die Originaldaten. Dies führt zur Forderung nach „sicheren“ Datentresoren oder zum Verfahren, die Medien „entfernt“ zu lagern.

Ein zweites Problem stellt ggf. die Vertraulichkeit der Daten auf den Backup-Medien dar: Gibt es Anforderungen an die Vertraulichkeit der Originaldaten (oder eines Teils davon), so überträgt sich diese Forderung auf die Backup-Medien. Als Lösung kommen in Frage

– die generelle Verschlüsselung der Daten auf dem Backup-Medium oder
– ein anderweitig gegen Verlust der Vertraulichkeit gesicherter Transport und eine entsprechende Aufbewahrung der Medien (z. B. in einem Tresor).

Man beachte, dass im zweiten Fall das Personal, das mit der Backup-Tätigkeit beauftragt ist, im Grunde Zugriff zu allen Daten auf dem Backup-Medium hat. Diese hohe Berechtigung ist aber für die Tätigkeit absolut unnötig und kann in der Praxis zu Problemen führen. Hier müsste in jedem Fall vertrauenswürdiges Personal zum Einsatz kommen – oder man erspart sich diese Probleme und nutzt die in den Backup-Systemen heute meist vorhandene Möglichkeit der Verschlüsselung. Es soll nicht unterschlagen werden, dass die Verschlüsselung andererseits oft mit einem erhöhten Zeitbedarf für die Durchführung des Backups erkauft wird. Es wird darüber hinaus ein Mindestmaß an Schlüsselmanagement erforderlich, da Schlüssel festgelegt, in das Backup-System auslesegeschützt eingebracht und ansonsten sicher archiviert (!) werden müssen. Letzteres ist erforderlich, um etwa nach einer brandbedingten Zerstörung des Backup-Systems mit einem anderen bzw. neuen Backup-System die Backup-Medien wieder lesen zu können.

Man erkennt hier wieder die alte Erfahrung in der IT-Sicherheit: Keine Lösung hat nur positive Eigenschaften, jeder Sicherheitsgewinn ist an anderer Stelle zu bezahlen…

Neben der Vertraulichkeit der Daten ist auch ihre Integrität zu diskutieren: Wenn schon ein Backup gezogen wird, sollen die Daten auch ihre Integrität behalten. Soweit es um das korrekte Schreiben der Daten auf das Medium geht, ist das Backup-System daraufhin zu prüfen, ob es z. B. fehlerkorrigierende Codes oder ähnliche Verfahren verwendet. Bei der Lagerung der Backup-Medien ist sicherzustellen, dass dies in geeigneter Umgebung passiert: Es macht keinen Sinn, etwa Backup-Tapes an Orten zu lagern, an denen mit hohen magnetischen Feldstärken zu rechnen ist. Datentresore sind z. B. daraufhin zu prüfen, ob sie eine geeignete Abschirmung leisten können.

Um die Problemschau abzurunden: Werden Backup-Medien aus dem Verkehr gezogen (z. B. wegen sich häufender Schreib- bzw. Lesefehler) ist ebenfalls das Problem der Vertraulichkeit der Daten zu beachten: Folglich sind die Datenträger entweder zu zerstören, wiederaufzubereiten (s. Abschnitt 11.4) oder sicher endzulagern.

Management-2

Wir fassen die Kernfragen zusammen:

– Wie ist die Vertraulichkeit der Daten auf dem Backup-Medium gesichert?

- Wie wird die Integrität der Daten auf dem Backup-Medium gewährleistet?
- Wo und wie können die Sicherungsmedien gelagert werden?
- Wann und wie sind Backup-Medien aus dem Verkehr zu ziehen?

11.9 System-Verfügbarkeit

Im Abschnitt über die Grundstrukturen haben wir das Thema „System-Verfügbarkeit" definitorisch behandelt.

Life-Cycle

Ein IT-System hat einen bestimmten Lebens-Zyklus, der mit seiner Entwicklung und Herstellung, der Auslieferung an den Kunden beginnt, dort über Konfiguration und Installation schließlich zum Betrieb führt (mit Unterphasen wie etwa Wartung und Update). Den Abschluss bilden die Phasen der Außerbetriebnahme und De-Installation.

Wir wollen hier nicht alle Phasen betrachten, weil dies den Rahmen sprengen würde. Zudem sind die Phasen der Entwicklung, Herstellung und Auslieferung von IT-Systemen selten im Einflussbereich des Anwenders. Dennoch seien folgende Hinweise gegeben:

Zertifizierung

Ein höheres Vertrauen, was die Phasen der Entwicklung, Herstellung und Auslieferung anbetrifft, erhält man dadurch, dass man Systeme einsetzt, die bezüglich ihrer Sicherheit zertifiziert sind. Die heute dazu verwendeten Sicherheitsstandards ITSEC und Common Criteria betrachten insbesondere auch den Life-Cycle eines Produktes oder Systems bis zur Auslieferung an den Kunden. Zertifizierung ist allerdings kein Allheilmittel, da man sehr genau darauf achten muss, *was* zertifiziert worden ist, und welche *Rahmenbedingungen* man im Betrieb einhalten muss, damit die Zertifizierung gültig bleibt. Bei letzterem tut man gut daran, sich den jeweiligen Zertifizierungsreport zu besorgen und die dort beschriebenen Verfahren und Hinweise genau einzuhalten.

Insbesondere ist zu beachten, dass Wartungsarbeiten mit Austausch oder Update von Hardware und Software schnell zum Verlust der Zertifizierung führen können. Man spricht deshalb auch davon, dass zertifizierte Systeme praktisch „eingefroren" bleiben müssen.

Wir halten fest, dass in Phasen der Entwicklung, Herstellung und Auslieferung von Systemen eine Fülle von Problemen vorhanden

sind, die sich mehr oder weniger in den späteren Phasen auswirken können: Fehler im Design und der Implementierung von Hardware und Software können zu Datenverlusten, zu reduzierter Verfügbarkeit, auch zu Fehlfunktionen von Sicherheitsvorkehrungen führen.

Betriebsphase

Beim Betrieb von IT-Systemen und Netzen muss man in Betracht ziehen, dass

- zufällige Defekte (ohne bekannte Ursache),
- Defekte in Folge von Alterung,
- Defekte aufgrund unzulässiger Umgebungsbedingungen (unzureichende Stromversorgung, Über- oder Unterschreiten von Klimabedingungen, Katastrophen wie Feuer, Wassereinbruch usw.),
- unzulässiges Verhalten von Personen (Unbefugte und Befugte)

zu Ausfällen oder verminderter System-Verfügbarkeit führen können.

System-Redundanz

Um Verluste zu begrenzen oder erst gar nicht entstehen zu lassen, ist natürlich die *Redundanz* von Systemen ein wichtiger Baustein. Dabei werden wichtige Hardware-Komponenten[50], ganze Systeme oder sogar vollständige Rechenzentren doppelt oder mehrfach vorgehalten. Bei Ausfall oder Fehlern wird manuell oder automatisch auf ein funktionstüchtiges Element umgeschaltet. Wichtig ist dabei meist die Umschaltdauer: Mit welchen Verzögerungen ist rechnen? Die Umschaltdauer sollte stets durch Tests ermittelt werden; das Umschalten auf ein redundantes System sollte regelmäßig „geübt“ werden, um die Tätigkeit als solche problemlos durchführen zu können, aber auch um abschätzen zu können, wie hoch ggf. die Verluste zeitlicher und betrieblicher Art sind.

Zur Behandlung der Alterungsprobleme sollte man sich einen Plan zurechtlegen, wann bestimmte Komponenten als Ersatz zu beschaffen und vorzuhalten, ggf. auszutauschen sind. In bestimmten Bereichen mag hierbei die Angabe des Lieferanten zur Mean Time Between Failure (MTBF) ein wichtiger Indikator sein.

---

50 Redundante Plattensysteme als Beispiel sind im Abschnitt 11.8 behandelt worden.

Um geeignete Umgebungsbedingungen zu etablieren und aufrechtzuerhalten sind eine ganze Reihe technischer Maßnahmen vorzusehen – hier nur einige Stichwörter: Paralleleinspeisung von elektrischer Energie, Notstromversorgung; Klimaanlagen einschließlich Klimaüberwachung; Brandmelde- und Löschsysteme. Es macht Sinn, sich beim Aufbau z. B. von Rechenzentren diese Punkte betreffend durch spezialisierte Firmen beraten zu lassen.

Eine andere Quelle für den Verlust oder die Minderung von System-Verfügbarkeit ist das Verhalten von Personen (Befugte wie auch Unbefugte). Eine Kontrolle des (*logischen*) Zugriffs und des (*physischen)* Zugangs zu IT-Systemen ist in jedem Fall erforderlich.

Zugriffskontrolle

Mit der Zugriffskontrolle kann man oft erreichen, dass *Unbefugte* die System-Verfügbarkeit nicht manipulativ oder unabsichtlich beeinträchtigen können.

Betriebsmittelbegrenzung

Der missbräuchlichen Vorenthaltung von Daten durch *Befugte* kann man in vielen Fällen mit einer Begrenzung der Betriebsmittel (verwendeter Speicherplatz, Anzahl laufender Prozesse und deren Prioritäten, CPU-Zeit, Anzahl von aufgebauten Verbindungen, usw.) entgegen wirken. Die Begrenzung der Betriebsmittel kann im Betriebssystem eines Rechners oder in den Applikationen integriert sein. Geht es um die Nutzung von Netzwerkdiensten, ist das *Load Balancing* ein geeignetes Mittel, um den *Denial of Service* zu erschweren, der darauf beruht, dass Netzwerkdienste überlastet werden, um deren Verfügbarkeit zu reduzieren oder sie vollständig zu blockieren.

Fernwartung

Unter den logischen Zugriff fällt auch die Fernwartung, die aus Sicherheitssicht als hochkritisch anzusehen ist, weil hiermit Befugten (meist solche mit hohen Rechten) Zugang zu den Systemen gewährt wird. Wichtige Fragen hierfür sind:

- Ist ein Fernwartungszugang unerlässlich oder kann man nicht darauf verzichten?
- Ist der Fernwartungszugang übertragungstechnisch abgesichert, d. h. findet eine Authentisierung statt und wird die Übertragung verschlüsselt und signiert betrieben?
- Erfolgt die Fernwartung ohne Kenntnis des System-Betreibers oder nur gegen Voranmeldung?
- Besteht für den Betreiber die Möglichkeit, die Wartung zu überwachen?

Die zuvor beschriebenen Probleme gelten natürlich nicht nur für das Thema Verfügbarkeit, sondern können auch für die anderen Sicherheitsziele (Vertraulichkeit, Integrität und vor allem auch missbräuchliche Nutzung) zu diskutieren sein.

Beim physischen Zugang zu Systemen sind verschiedene Personengruppen zu betrachten:

Reinigungspersonal

Reinigungspersonal benötigt Zutritt zu Räumlichkeiten mit IT-Systemen, wird dennoch eher selten bei seiner Tätigkeit überwacht, obwohl dies relativ leicht möglich wäre. Es muss dabei gar nicht unbedingt um ein Manipulationsszenario gehen – es reicht schon aus, wenn durch unsachgemäße Handhabung Defekte an Systemen provoziert werden.

Wartungspersonal

Beim Wartungspersonal ist die Lage etwas schwieriger: Man kann zwar eine Aufsicht führen, ist jedoch bei den Wartungstätigkeiten nur beschränkt in der Lage, jeden einzelnen Schritt zu überwachen und auf Korrektheit und Zulässigkeit zu prüfen. Dennoch sei darauf hingewiesen, dass in Systemen mit hohem Sicherheitsbedarf ein ausgereiftes Kontroll- und Aufsichtsverfahren unabdingbar ist.

Besucher

Sofern Besuchern überhaupt Zutritt zu IT-Räumlichkeiten gewährt wird, ist darauf zu achten, dass diese

- als Besucher kenntlich sind (Plakette),
- vorher über sicherheitsgerechtes Verhalten unterrichtet werden,
- Zutritt und Verlassen der Räumlichkeiten protokolliert werden,
- sich grundsätzlich nicht ohne Aufsicht bewegen dürfen.

Betrachten wir noch einige andere Konzepte zum Thema System-Verfügbarkeit:

Betriebsbereitschaft

Für IT-Systeme kann man die *Betriebsbereitschaft* (*Continuity of Service)* betrachten: Dabei geht es darum, eine Wahrscheinlichkeit für die Betriebsbereitschaft zu garantieren – etwa in der Art "Über einen Zeitraum von einem Jahr wird Betriebsbereitschaft zu 99,99 % der Zeit zugesichert".

Für extrem hohe Anforderungen an die Betriebsbereitschaft sind so genannte *NonStop*-Systeme auf dem Markt erhältlich. Sie zeichnen sich u. a. dadurch aus, dass technische Komponenten (Prozessoren, Speicher, Übertragungskanäle) hoch redundant ausgelegt sind; weiterhin ist es möglich, Wartung im laufenden

Betrieb durchzuführen und technische Komponenten auswechseln zu können, ohne irgendeinen Absturz oder Datenverlust zu provozieren. Dies geht sogar so weit, dass einzelne CPUs „gezogen“ werden können, da durch kombinierte Hard- und Software-Maßnahmen sichergestellt ist, dass andere CPUs diesen Vorgang erkennen und die laufenden Tasks sofort übernehmen.

Ein anderer methodischer Zugang zu dem Problem der System-Verfügbarkeit bietet die Betrachtung der Funktionen[51] *Rechtzeitigkeit*, *Fehlererkennung*, *Fehlerüberbrückung* und *Fehlerbehebung*:

Rechtzeitigkeit

Es kann entscheidend sein, dass eine gewünschte Funktion oder Dienstleistung innerhalb einer akzeptierten Zeit oder zu einem bestimmten Zeitpunkt erbracht wird. Diese Anforderung bezeichnen wir als *Rechtzeitigkeit*. Die Rechtzeitigkeit kann beeinträchtigt sein, wenn

- zeitkritische Aufgaben nicht genau zu dem Zeitpunkt durchgeführt werden können, zu dem es erforderlich ist,
- zeitunkritische Aufgaben in zeitkritische umgewandelt werden können,
- Betriebsmittel unnötig angefordert oder zurückgehalten werden.

Es sind folgende Kernfragen zu stellen:

- Welche Funktionalität ist mit welcher *Priorität* zu gewährleisten?
- Welche *Reaktionen* des Systems müssen in welcher Zeit erfolgen?
- Welche Betriebsmittel müssen in welchem Umfang und zu welchem Zeitpunkt zugänglich sein?
- Unter welchen *Randbedingungen* ist die betreffende Funktionalität einzuhalten?

IT-Systeme, die die Rechtzeitigkeit von Verarbeitungen garantieren können, werden *Echtzeit-Systeme (Real-Time Systems)* genannt. Die zugehörigen Betriebssysteme besitzen bestimmte Me-

---

51 In Sicherheitskriterien wie den ITSEC und den Common Criteria werden diese Teilfunktionen unter den Begriffen *Gewährleistung der Funktionalität* oder *Zuverlässigkeit der Dienstleistung* (Reliability of Service) zusammengefasst.

chanismen zur Verteilung der Prozessor-Zeit (Scheduling) und der Steuerung von Prioritäten, sowie die Verriegelung und Freischaltung von Verarbeitungen. Echtzeit-Systeme werden typischerweise bei der Steuerung kritischer Prozesse (Produktion, Überwachung) eingesetzt.

Fehlererkennung

Fehlererkennung meint, dass Fehler an der Quelle oder zu einem möglichst frühen Zeitpunkt an ihren Auswirkungen erkannt werden. Bei der Fehlererkennung sind die Aspekte der *Vollständigkeit* und *Korrektheit* der Fehleranalyse zu betrachten; es ist wichtig festzulegen, *welche* Fehler unbedingt erkannt werden müssen.

Vor allem in Systemen der höheren Preisklassen sind viele technische Komponenten mit automatischen Prüfeinrichtungen versehen, so dass sporadische oder auf Defekten beruhende Fehler erkannt (und teilweise automatisch korrigiert werden können). Einfachste Beispiele hierfür sind Parity-Prüfungen und fehlerkorrigierende Codes.

Fehlerüberbrückung

Unter Fehlerüberbrückung *(Error Recovery)* versteht man das Vermeiden weiteren Fehlverhaltens oder das Begrenzen der Auswirkungen des Fehlverhaltens eines Systems. Die Fehlerüberbrückung kann einen *kontrollierten* Abbruch oder den Versuch einer *Fehlerkorrektur* beinhalten. Es spielen dabei folgende Einzelaspekte eine Rolle:

- Welche Beeinträchtigungen – z. B. Daten-, Funktions- oder Zeitverlust – können in Kauf genommen werden?
- Welche Fehlerklassen sollen überbrückt werden?
- Wie soll die Fehlerüberbrückung erfolgen?

Bei Auftreten von Fehlerzuständen – nicht nur der Hardware, sondern auch bei den bekannten, meist nicht nachvollziehbaren Systemabstürzen – kann vielfach eine Kopie des Arbeitsspeichers und weiterer wichtiger Daten auf einen externen Speicher geschrieben werden (Checkpoint, Dump). Danach erfolgt ein kontrollierter Abbruch. Nach Behebung möglicher Hardware-Fehler können Diagnose-Programme anhand dieser Kopie weitere Fehlerursachen und die Fehlerauswirkungen analysieren. Das Ergebnis kann zu

- einem Zurücksetzen des Systems und einem Neustart mit Verlust aller laufenden Tasks (Worst Case),
- einem Wiederaufsetzen auf einen früheren Stand (Backward Recovery), oder

– einem Wiederaufsetzen auf einen zukünftigen, korrekten Stand (Forward Recovery) führen.

Fehlerbehebung

Die Fehlerbehebung ist dafür zuständig, erkannte Fehler an der Quelle zu beheben, so dass anschließend die Verarbeitung möglichst verlustfrei weitergeführt werden kann. Vielfach reduziert sich das Problem darauf, defekte Komponenten manuell auszutauschen, Daten wiedereinzuspielen oder Ersatzsysteme in Betrieb zu nehmen. Einige Fälle der *automatischen* Fehlerbehebung haben wir schon genannt.

11.10 Übertragungssicherung

Der Sicherheit von Daten auf Übertragungswegen kommt eine hohe Bedeutung zu. Unter *Übertragungswege* fallen hier klassische Leitungen, aber auch Funkstrecken, optische und akustische Verbindungen. Bei der Sicherheit der Datenübertragung spielen alle Ziele der Vertraulichkeit, Integrität, Verfügbarkeit und Verhinderung von Missbrauch eine Rolle. Die Sicherheit ist generell bedroht durch

– unbefugte Kenntnisnahme von Daten (Abhören),
– unbefugtes bzw. unerwünschtes Ändern von Daten,
– unbefugte Inanspruchnahme von Dienstleistungen der Übertragung (bis hin zum *Denial of Service*),
– unbefugtes Einspielen von Daten (*Replay-Attacken*),
– Ausfall von Übertragungsdiensten und -strecken.

In einer erweiterten Betrachtung haben wir das Ziel der *Verbindlichkeit* der Kommunikation zu betrachten. Diesem Ziel können das

– Leugnen von Kommunikationsbeziehungen,
– das Nichtanerkennen von Daten und
– das Leugnen des Empfangens und Absendens

zuwider laufen.

Sicherheitsfunktionen, die solche Bedrohungen abwehren, fasst man oft unter der Überschrift *Übertragungssicherung* zusammen. Wir haben einige wesentliche Methoden der Übertragungssicherung in den vorausgehenden Abschnitten behandelt:

– Verschlüsselung verhindert unbefugte Kenntnisnahme.
– Signaturen lassen unbefugtes Ändern von Daten erkennen.

- Zertifikate ermöglichen das Authentisieren von Personen und IT-Systemen.
- Redundante Übertragungskanäle (Leitungsführung, Funkstrecken) bzw. redundante Übertragungsdienste (z. B. Nutzung von 2 Providern für den Internet-Zugang) sind Methoden, um die Verfügbarkeit zu erhöhen.

Load Balancing

Denial of Service Attacken, bei denen Netzwerkdienste auf bestimmten Rechnern überlastet werden sollen, können durch Einsatz von Load Balancing zwar nicht verhindert, aber in ihren Auswirkungen begrenzt werden.

Verkehrsanalyse

Bei Netzwerken stellt sich die Frage, ob neben den Nutzdaten auch Adressdaten (und ergänzende Informationen wie z. B. Protokollinformationen) vertraulich bleiben sollen. Mithörer sind andernfalls in der Lage, eine Verkehrsanalyse durchzuführen: Aus dem „Verkehrsaufkommen" zwischen zwei Kommunikationspartnern (z. B. plötzlich auffällig häufiger Datenaustausch) kann ein Dritter durchaus seine Schlüsse ziehen...

Solche Aspekte werden typischerweise in Funknetzen betrachtet. In leitungsgebundenen Datennetzen mit verschlüsselten Adressdaten müssten die Router im Netz Kenntnis des Schlüssels haben und über Möglichkeiten des Ver- und Entschlüsselns verfügen.

11.11 Beweissicherung und Auswertung

Hier begegnen wir der Aufgabe, für bestimmte Zwecke (Sicherheits-)Nachweise generieren und bei bestimmten Anlässen auswerten zu können. Als Nachweise kommen in unserem Kontext nur schriftliche Aufzeichnungen (Protokolle, Snapshots, Fotos,…) in Betracht.

Accounting

Das Erzeugen und Sicherstellen von Nachweisen wird im Englischen als *Accounting* bezeichnet. Auch wenn es banal erscheint: Ziel der Beweissicherung ist es, Beweise zu sichern. Beweischarakter haben Daten dann, wenn sie objektiv erhoben und datierbar sind und möglichst bestimmten Subjekten zugeordnet werden können. Dazu ist es offensichtlich erforderlich, dass die Identität der Subjekte zweifelsfrei feststeht, d. h. eine Authentisierung stattgefunden hat. Weiterhin muss ausgeschlossen werden, dass Beweise nachträglich gelöscht, verfälscht oder vorgetäuschte Nachweise eingefügt werden können.

Im Zusammenhang mit der Sicherheit geht es meist um die Aufzeichnung bzw. Protokollierung der versuchten und / oder tatsächlichen Ausübung von Rechten. Typische Beispiele für solche

Funktionen sind das Eintragen von Besuchern in eine Liste (Betreten und Verlassen von Sicherheitsbereichen), Listen über Betreten und Verlassen solcher Bereiche durch Befugte, Mitschreiben von Log-in-Vorgängen bei IT-Systemen („Log-Protokolle“), Protokolle über unzulässige Zugriffsversuche oder unzulässigen Verbindungsaufbau.

Management

Wichtige Einzelfragen sind:

– Welche Aktionen sind zu protokollieren?

– Welche Informationen sind dabei jeweils aufzuzeichnen?

Um Beweischarakter zu erreichen, müssen Datum und Uhrzeit, möglichst die Identität des Verursachers und der genaue Vorgang erfasst werden.

– Werden die Aktionen *aller* Subjekte aufgezeichnet?

Werden Aktionen bestimmter Subjekte nicht aufgezeichnet, besteht die Gefahr, dass Unbefugte sich unter dieser Identität (etwa durch Beschaffung des Passwortes) tarnen und somit keine Spuren ihrer Aktivitäten hinterlassen. Ein attraktives, weil hoch privilegiertes Ziel ist dabei natürlich die Rolle eines System-Administrators.

– Wo werden die Aufzeichnungen gespeichert bzw. aufbewahrt?

Da Protokolle viel Speicherplatz benötigen, stellt sich generell die Frage, was passiert, wenn der zur Verfügung stehende Speicherplatz erschöpft ist? Die sicherste, aber meist nicht praktikable Lösung besteht darin, keine weiteren Aktionen zuzulassen, das System zu stoppen und diesen Zustand nur durch den System-Administrator nach Sicherung der Protokoll-Daten z. B. auf einem externen Medium aufheben zu lassen. Die weniger "brutale" Lösung ist, einige Zeit vor dem Speicherüberlauf Warnmeldungen zu geben, die wiederum den System-Administrator auf den Plan rufen müssen.

Die Lösung „das System läuft einfach ohne Protokollierung weiter“ (und dies dann meistens sogar schneller) ist aus Sicht der Sicherheit bedenklich: Es werden keine Beweise mehr gesichert; dies könnte sogar manipulativ ausgenutzt werden, indem man vor bestimmten Aktionen erst einmal das Accounting zum Überlauf bringt.

– Wer hat Zugriff auf die gespeicherten Aufzeichnungen?

- Sind für die Aufzeichnungen Vertraulichkeit, Verfügbarkeit, Integrität und Missbrauchsschutz gewährleistet?
- Wann werden Aufzeichnungen gelöscht bzw. überschrieben?

Auswertung, Audit

Kommen wir zur zweiten Funktion bzw. Maßnahme: der (Protokoll-)Auswertung. Das Auswerten von Nachweisen wird im Englischen *Audit* genannt. Hier geht es darum, bei bestimmten Gelegenheiten aus den vorhandenen Aufzeichnungen Schlüsse zu ziehen. Ein solcher Anlass kann ganz banal die Abrechnung der Nutzung bestimmter Betriebsmittel (z. B. im Rahmen von Kunden-Projekten) sein – aber eben auch ein vermuteter Sicherheitsvorfall oder -verstoß, den man nachträglich nachvollziehen möchte. Die Protokoll-Auswertung "erfährt" Sicherheitsverstöße naturgemäß erst dann, wenn sie bereits passiert sind.

Intrusion Detection

In der Kombination mit einem Sicherheitsalarm kann man immerhin dafür sorgen, dass ein Vorfall nicht über längere Zeit „unentdeckt“ bleibt. Damit sind wir im Grunde schon bei einem technischen System, das genau diese Funktion ausführt – dem IDS (*Intrusion Detection System*).

Ein generelles Problem aller von IT-Systemen erzeugten Aufzeichnungen ist ihr Umfang und in der Folge die Unübersichtlichkeit der Daten. Die Erfahrung, dass vielfach umfangreich protokolliert, aber nie ausgewertet wird, mag hierauf zurückzuführen sein. Hier geht es nicht ohne entsprechende Werkzeuge, mit denen die Aufzeichnungen nach bestimmten Merkmalen und Zusammenhängen untersucht werden können.

Management

Die Schlüsselfragen zur Auswertung sind:

- Bei welchen Anlässen wird eine Auswertung vorgenommen?
- Wer wertet Aufzeichnungen aus?
- Nach welchen Kriterien wird die Auswertung vorgenommen?
- Welches Verfahren der Auswertung wird angewendet (z. B. mittels eines Werkzeugs oder – wo sinnvoll – manuell)?
- Welche Maßnahmen schließen sich an die Entdeckung eines fraglichen Vorfalls an?
- Werden Vorbeugemaßnahmen abgeleitet, um zukünftig vergleichbare Vorfälle auszuschließen?

Eine wichtige Frage ist, ob die Aufzeichnung und die Auswertung bestimmter Daten über das Handeln von Personen z. B. vor dem Hintergrund des Datenschutzes überhaupt zulässig ist. Können Aufzeichnungen vielleicht sogar zur verdeckten Leistungskontrolle von Mitarbeitern dienen? Hier empfiehlt sich, solche Fragen mit dem Datenschutzbeauftragten und der Mitarbeitervertretung vorab – schon bei der Erstellung des Sicherheitskonzeptes – zu klären.

Das (längerfristige) Speichern von Verbindungsdaten in öffentlichen Netzwerken ist unter Datenschutzgesichtspunkten ebenfalls ein heißes (politisches) Diskussionsthema.

Non Repudiation

Bei der Sicherheit von Geschäftsprozessen haben wir die Verbindlichkeit der Kommunikation zwischen Partnern als wichtiges Ziel diskutiert. Dabei geht es auch darum, dass der Empfänger den Empfang von Daten nicht nachträglich leugnen kann *(Non Repudiation)*. Dazu können natürlich Verfahren der Protokollierung und Auswertung ebenfalls hilfreich sein.

12 Sicherheit im Internet

Nach diversen ersten Ideen und Netzwerk-Konzepten entstand im Jahr 1969 das erste Internet als Verbindung und Kommunikation von mehreren Computern unter dem Namen ARPANET: Per Telefonleitung wurden vier Großrechner an verschiedenen Universitäten und Instituten der USA miteinander verbunden und als erstes Datenpaket wurde das Wort "Login" übermittelt.

Es folgte 1972 die Erfindung der Email-Kommunikation mit einer heute noch gültigen Adressstruktur und 1973 die Verwendung des universellen Transportprotokoll-Standards TCP/IP.

In dieser Zeit kannten sich die wenigen Entwickler, die gleichzeitig auch die Rolle der Benutzer einnahmen, persönlich untereinander und verzichteten auf Sicherheitsmechanismen wie Authentifizierung und Verschlüsselung. Man war ja sozusagen unter sich. Das hat sich bis heute nicht geändert, nur dass sich der Teilnehmerkreis mit über einer Milliarde Internetbenutzer drastisch erweitert hat.

Der endgültige Durchbruch zum Business- und Massenmedium begann, nach freigegebener Kommerzialisierung 1990, etwa ab 1995 mit langsam einsetzenden Internetmarketing / e-commerce und dem forcierten Vertrieb von privaten Internetzugängen. In dieser Zeit entstanden heutige Global Player wie Yahoo, ebay oder Amazon.

Nach ca. 160.000 Hosts[52] im Jahre 1989, waren nur 5 Jahre später bereits rund 4 Millionen Hosts registriert.

Per se ist das Internet völlig unsicher. Ohne zusätzliche Vorkehrungen werden alle Daten unverschlüsselt übertragen und die Datenquellen und -senken sind nicht authentifiziert.

Internet-Dienste

Betrachtet man die Internet angebotenen Dienste wie World Wide Web (WWW), E-Mail, Internet-Telefonie (VoIP), etc. ergeben sich weitere Sicherheitsprobleme.

---

52 Host = Internetserver

Die wichtigsten Schwächen – vorweg gesagt – sind mangelhafte Konzeption und Fehler, die durch eine falsche Konfiguration oder fehlerhafte Programmierung entstehen.

Will man nicht das erfolgreiche Konzept eines flexiblen Netzes zum freien Informationsaustausch zerstören, so ist es dringend nötig, die vorhandenen Möglichkeiten zur Verbesserung der Sicherheit zu nutzen und weiterzuentwickeln sowie vor allem auch die Benutzer über die Gefahren aufzuklären.

12.1 Gefährdungen

Durch die Tatsache, dass jeder Benutzer den Umgang mit dem Medium Internet zum großen Teil selbst gestaltet und zu verantworten hat, ist die Aufklärung der Benutzer – über die erheblichen, aber dennoch zum größten Teil vermeidbaren Gefährdungen – für die Verwendung des Internets bei der betrieblichen Tätigkeit von großer Bedeutung.

Dabei müssen für die Verwendung des Internets am Arbeitsplatz die Sicherheitsanforderungen für den Benutzer in Form von Regeln und eingesetzter Technik klar vorgegeben werden.

Wir werden nun die wesentlichen Gefährdungen bei den gebräuchlichsten Verwendungen des Internets am Arbeitsplatz näher diskutieren.

World Wide Web

Der beliebteste Dienst im Internet ist das World Wide Web (WWW). Sehr einfach zu bedienende Clientsoftware, der so genannte Browser, ermöglicht den Zugriff auf Informationen mit Hilfe des HyperText Transfer Protocol (HTTP).

HyperText

Unter *HyperText* versteht man die Möglichkeit, unterschiedliche Daten, also z. B. auch Graphiken, Filme und Tondateien für einen leichten Zugriff miteinander zu verknüpfen.

Das WWW ermöglicht mittlerweile den Zugriff auf ein gigantisches Informationsangebot, das bei der betrieblichen Tätigkeit den Besuch von Bibliotheken zum Nachschlagen von Informationen fast völlig obsolet hat werden lassen.

Allerdings werden im WWW auch alle Arten von Pornographie sowie Webseiten mit rassistischen und fanatisch religiösen Inhalten angeboten, deren Aufruf bei einem betrieblich genutzten Internetzugang nicht zu tolerieren ist (Jugendschutzgesetz, Allgemeines Gleichstellungsgesetz etc.).

Weiter kann der Besuch solcher Webseiten zu einer unerwünschten Funktionserweiterung des Browsers durch Schadsoftware führen; es kann bereits ausreichen, eine Webseite nur in einem dafür anfälligen Browser aufzurufen, um sich zum Beispiel einen Trojaner einzufangen.

Betriebliche Regeln

Hier hat die Geschäftsführung zusammen mit dem Security Manager klare Regeln zu erlassen, wie die betriebliche Verwendung des WWW zu erfolgen hat. Diese Regeln müssen kommuniziert sowie deren Einhaltung in Abstimmung mit dem Betriebsrat zyklisch überprüft werden.

E-Mail

Elektronische Post mit ihren vielen Vorteilen ist sicherlich einer der populärsten Dienste innerhalb von Computer-Netzen.

SPAM

Leider werden E-Mails auch zur Versendung unerwünschter Massensendungen verwendet, die unter dem Namen "SPAM" (der Name rührt von einem Sketch der englischen Komikertruppe "Monty Python" her) bekannt sind. Über ihre Anhänge – meist aus Office-Software stammend – kann Schadsoftware wie Computerviren, Würmer und Trojaner in die Endgeräte eingeschleust werden.

Eine wesentliche Gefährdung geht auch von der Tatsache aus, dass keine Authentisierung zwischen den Partnern einer Mailübertragung stattfindet, so dass prinzipiell jeder Benutzer Nachrichten mit einer falschen Absenderangabe verschicken kann, die im Klartext übertragen wird.

Der Verlust der Authentizität und Vertraulichkeit lässt sich durch den Einsatz von geeigneten Verschlüsselungsverfahren verhindern, wobei allerdings immer noch die Gefahr einer Verkehrsflussanalyse gegeben ist.

Ein unverschlüsselt im Internet stattfindender Mailverkehr ist mit dem Versand nicht unterschriebener Postkarten zu vergleichen.

Offener Datenaustausch im Internet

Eine weitere Gefährdung bei der Benutzung des Internet stellen der Verlust der Vertraulichkeit durch ein Mitlesen der versandten Daten und der Verlust der Integrität durch die Manipulation der Daten dar.

Viele der im Internet benutzten Dienste übertragen die Benutzernamen und Passwörter offen, so dass jeder, der privilegierten

Zugang zu einem der an der Übertragung beteiligten Gateways, Router oder Server hat, diese Daten lesen oder verändern kann.

Replay

Das Mitlesen der versandten Daten ermöglicht auch so genannte *Replay Attacks*, bei denen einmal zur Authentisierung benutzte Daten, wie z. B. verschlüsselte Passwörter, von einem Angreifer bei einem späteren Zugangsversuch wieder eingespielt werden.

TCP/IP

Da sehr häufig beim TCP/IP Protokoll die Authentisierung der Rechner nur über die IP-Adresse erfolgt, wird durch Fälschen der IP-Adresse, dem sogenannten IP-Spoofing, ein unberechtigter Zugang möglich. Die Authentifizierung über die IP-Adresse findet man häufig bei mobilen Endgeräten und sollte dringend durch eine sichere Methode, z.B. mit Zertifikaten und Smartcards, ersetzt werden.

IPv6

Heute findet überwiegend die Version 4 des TCP/IP Protokolls (IPv4) Verwendung. Die erweiterte Version des IP Protokolls (IPv6) hat neben der Erweiterung des Adressraums auch eine Verbesserung des Schutzes der übertragenen Daten in Form von zusätzlichen Headern (Kopfdaten) zu bieten. Eine Überprüfung von Integrität und Authentizität ist mit Hilfe des Authentication Header möglich; die Verschlüsselung privater Daten erfolgt mit Hilfe des Privacy Header.

Für einen umfassenden Einsatz im Internet ist allerdings ein weltweit einheitliches Schlüsselmanagement erforderlich. Aber schon lokale Lösungen z. B. auf der Basis des Standards X.500 sind ein wesentlicher erster Schritt, um den Benutzern Vertrauen in eine elektronische Kommunikation mit unbekannten Partnern zu geben.

Es gibt darüber hinaus noch zahlreiche weitere Angriffsmöglichkeiten auf die Endgeräte, Router, DNS Server etc. im Internet, die durch Schwachstellen in der Software und in den Protokollen bedingt sind, auf die wir aber wegen des sehr speziellen Charakters nicht näher eingehen wollen.

12.2 Schutzmaßnahmen: Regelwerke für Internet und E-Mail

Wesentliche Schwachstellen bei der Verwendung von Internetzugängen und E-Mail lassen sich durch organisatorische Regelungen, die von der Geschäftsleitung kommuniziert werden, vermeiden.

Regelwerke

Insbesondere ist zu regeln

– der Gebrauch des Internet-Zugriffs für betriebliche Zwecke,

- das private Surfen über den betrieblichen Internet-Zugang,
- das Herunterladen von Dateien, Software und Informationen (Text, Bilder, Videos und Tonmaterial),
- die Verwendung des betrieblichen E-Mail Systems, Versendung von E-Mails privater Natur,
- der Umgang mit gespeicherten E-Mails und die Verwendung von Archivierungsmöglichkeiten,
- der Umgang mit falsch adressierten bzw. irrtümlich empfangenen E-Mails,
- der Umgang mit Internet-Suchmaschinen.

12.3 Technische Schutzmaßnahmen: Internet-Firewalls

Eine (Internet) Firewall ist eine Anordnung von Hard- und Software, die als alleiniger Übergang zwischen zwei zu trennenden TCP/IP Netzen dient, von denen das eine einen höheren Schutzbedarf hat.

Firewall Policy

Für eine Firewall Policy sind folgende Punkte zu beachten:

- Ein Firewall hat nur diesen Zweck: Auf dem entsprechenden System dürfen keine weiteren Dienste implementiert sein.
- Ein Zugang zur Firewall darf nur über eine gesicherte Verbindung aus dem Intranet des Unternehmens möglich sein.
- Die Konfiguration baut auf einer für das zu schützende Netz definierten Security Policy auf und gestattet nur die dort festgelegten Verbindungen.
- Diese Verbindungen müssen nach IP-Adresse, Dienst und Benutzer getrennt festgelegt werden können.
- Alle korrekt aufgebauten Verbindungen *müssen* protokolliert werden, alle abgewiesenen *sollten* protokolliert werden.
- In der Firewall Policy muss festgelegt werden, welche Dienste für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Dienste Vertraulichkeit und/oder Integrität gewährleistet werden müssen. Alle anderen Dienste werden verboten!

– Es muss festgelegt werden, ob und welche der übertragenen Nutzinformationen gefiltert werden sollen (z. B. Kontrolle auf Computer-Viren).
– Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet.

Die Firewall Policy sollte so beschaffen sein, dass sie auch zukünftigen Anforderungen gerecht wird, d.h. es sollte eine ausreichende Anzahl von Verbindungsmöglichkeiten vorgesehen werden. Jede spätere Änderung muss streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden. Die Firewall Policy ist regelmäßig zu überprüfen (z.B. durch interne Audits)

Ausnahmeregelungen insbesondere für neue Dienste und kurzzeitige Änderungen (z. B. für Tests) sind stets schriftlich zu beantragen und einem Genehmigungsverfahren zu unterziehen.

Risiko-Abschätzung

Für eine Risiko-Abschätzung müssen folgende Fragen geklärt werden:

– Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn die Firewall durchbrochen oder zerstört wird? Ist dieser Schaden tragbar (absolute Sicherheit gibt es nicht!)?
– Welche Restrisiken existieren bei einem ordnungsgemäßen Betrieb der Firewall? Dies sind z. B. Schwachstellen in den benutzten Geräten und Betriebssystemen.
– Wie schnell wird ein Angriff auf die Firewall bemerkt?
– Welche Protokoll-Informationen sind auch nach einem erfolgreichen Angriff noch verfügbar?
– Sind die Benutzer bereit, die Einschränkungen durch die Firewall zu akzeptieren?

Unterschiedliche Arten von Firewalls: Packet Filter

Packet Filter

Packet Filter sind Router oder Rechner mit spezieller Software, welche die in den Schichten 3 und 4 der TCP/IP Protokollfamilie (IP, ICMP, ARP, TCP und UDP) vorhandenen Informationen zum Filtern der Pakete benutzen. Hierzu werden Access- bzw. Deny-Listen benutzt.

Folgende Forderungen sind gemäß /BSI-M/ an Packet Filter zu stellen:

– Die Filterung muss getrennt für jedes Interface möglich sein.

- Die Filterung muss getrennt nach Quell- und Zieladresse für einzelne Rechner oder für komplette Teilnetze möglich sein.
- Die Filterung muss getrennt nach Quell- und Zielport möglich sein.
- Die Reihenfolge der Filterregeln darf nicht automatisch vom Packet Filter verändert werden.
- Wenn mehr als zwei Interfaces vorhanden sind, muss eine Filterung getrennt für ankommende und ausgehende Pakete möglich sein.
- Die Eingabe und Kontrolle der Filterregeln muss einfach und übersichtlich sein, z. B. durch symbolische Angabe von Dienst- und Protokollnamen.
- Bei TCP-Paketen muss eine Unterscheidung möglich sein, ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird.
- Es muss eine Protokollierung von Hardware-Adresse, IP-Adresse, Dienst, Zeit und Datum für jedes Paket stattfinden, wobei auch Einschränkungen auf bestimmte Pakete (z. B. nur Pakete mit einer speziellen Quell-Adresse) möglich sind.
- Sämtliche Protokollinformationen müssen an einen externen Host zur Logfile-Archivierung und -analyse geschickt werden können.

Unterschiedliche Arten von Firewalls: Application-Gateway

Application Gateway

Ein Application Gateway ist ein Rechner, der die in der Anwendungsschicht vorhandenen Informationen zum Filtern von Paketen oder Verbindungen nutzt.

Dies können z. B. Benutzernamen in Verbindung mit einer starken Authentisierung, spezielle Informationen in den übertragenen Daten (z. B. Kontrolle auf Computer-Viren) oder spezifizierten Informationen der Anwendungsschicht sein.

Ein Application Gateway bietet darüber hinaus die Möglichkeit, einen einheitlichen Zugang zum zu schützenden Teilnetz zu schaffen und die Struktur dieses Netzes zu verdecken. Die auf dem Application Gateway laufenden Filter-Prozesse werden als Proxy Server bezeichnet.

Folgende Forderungen sind gemäß /BSI-M/ an Application Gateways zu stellen:

- Es müssen alle wesentlichen Protokolle der Anwendungsschicht behandelt werden.
- Für jedes unterstützte Protokoll muss eine Filterung nach spezifizierten Informationen möglich sein. Insbesondere müssen die Filterregeln benutzerabhängig formulierbar sein, und es muss möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.
- Es muss eine Filterung nach der in der Security Policy festgelegten Nutzinformation möglich sein (z. B. Kontrolle auf Computer-Viren).
- Bei dem Einsatz eines Application Gateways sollte keine Änderung der Software im zu schützenden Netz oder im unsicheren Netz nötig sein.
- Die Eingabe und Kontrolle der Filterregeln muss einfach und übersichtlich sein.
- Die eingesetzten Programme müssen gut dokumentiert sein.
- Es muss leicht möglich sein, neue Protokolle hinzuzufügen.
- Für jede aufgebaute und abgewiesene Verbindung muss eine Protokollierung von Benutzer-Identifikation, IP-Adresse, Dienst, Zeit und Datum durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen (z. B. für einen speziellen Benutzer) möglich sind.
- Die Protokollinformationen müssen an einen externen Host zur Logfile-Archivierung und -analyse geschickt werden können.
- Zur Benutzer-Identifikation müssen starke Authentisierungsmethoden unterstützt werden.

Weitere Schutzmaßnahmen

Weitere technische Schutzmaßnahmen sind Intrusion Detection und Intrusion Prevention Systeme (IDS, IPS), die in der Regel aber sehr schwer zu konfigurieren sind und für ihren Betrieb einen nicht unerhebliche Menge geschulten Personals benötigen.

12.4 Zusammenfassung

Internet-Sicherheit ist ein nicht unerheblicher, komplexer Teil der IT-Sicherheit einer Organisation, den wir nur in einigen wichtigen Aspekten betrachten konnten. Abschließend wollen wir noch folgendes festhalten:

- Prinzipiell ist eine funktionierende Sicherheit beim Umgang mit dem Internet keine Frage, die ein einzelner Mitarbeiter für seinen Arbeitsplatz beantworten kann, sondern Internet-Sicherheit kann nur funktionieren, wenn sie ganzheitlich geplant wird.
- "Ganzheitlich" bedeutet insbesondere, dass alle betroffenen Abteilungen in diesen Prozess eingebunden werden müssen, einschließlich Vertreter der Geschäftsleitung, die schlussendlich auch die einzelnen Schritte absegnen muss.

Letzteres ist auch im Sinne der Mitarbeiter: Man denke hier beispielsweise an die Suche nach einem Verantwortlichen (oder Opfer) bei einem Sicherheitsvorfall, der zu Konsequenzen für den Mitarbeiter führen kann, wenn die Verantwortlichkeiten und Regeln bei dem betrieblichen Umgang mit dem Internet nicht von vorneherein klar definiert sind.

13 Infrastruktursicherheit

In diesem Kapitel wollen wir uns mit den Sicherheitsaspekten beschäftigen, die mit den Besonderheiten der Umgebung, in der schützenswerte Daten verarbeitet werden, zu tun haben. Schutzmaßnahmen entstammen hier überwiegend aus der Bauphysik, dem Einschließen und Überwachen; daher der Name physische Sicherheit.

Physische Sicherheit dürfte die älteste angewendete Sicherheitsform sein. Von jeher wurden Wertgegenstände in sicheren Behältnissen verwahrt und bewacht. In den Anfangszeiten der Datenverarbeitung wurde diese Sicherheitsform einfach adaptiert. Dazu wurden die Geräte und Medien zur Informationsverarbeitung und -speicherung in sicheren Schränken oder Räumen in Rechenzentren verwahrt und diese bewacht. Im Zeitalter der globalen Kommunikation und den nach dem Client-Server-Schema verteilten Applikationen reicht physische, umgebungsbezogene Sicherheit allein natürlich nicht aus; sie ist aber in vielen Fällen eine kostengünstige, praktikable Alternative oder Ergänzung.

13.1 Geltungsbereiche und Schutzziele

Festlegung der Sicherheitszonen

Zu schützende Bereiche können etwa Rechnerräume, Räume mit Peripheriegeräten (Drucker, etc.), Archive, Kommunikationseinrichtungen und die Haustechnik sein. Solche Sicherheitszonen können unterschiedlich hohen Sicherheitsbedarf aufweisen.

Die Überwachung des Zutritts zu Gebäuden, Rechenzentren und sicherheitssensiblen Geräten, allgemein zu Sicherheitszonen, zählt zu den wichtigsten physischen Schutzmaßnahmen. Das *Zutrittskontrollsystem* beinhaltet verschiedene bauliche, organisatorische und personelle Maßnahmen.

Management

Beim Management der Zutrittskontrolle sind die generellen Richtlinien für den Umgebungs-, Gebäude- und Geräteschutz festzulegen. Dabei sind folgende Fragen zu klären:

- Wer darf Zutritt zu einem Sicherheitsbereich haben?
- Wann darf die Person Zutritt zu dem Sicherheitsbereich haben?

- Zu welchen (Teil-)Bereichen darf eine Person Zutritt haben?
- Wer hat den Zutritt gestattet?
- Wie wird der Zutritt kontrolliert?

Perimeterschutz

Neben dem Gebäudeschutz ist der Perimeterschutz, auch Freilandschutz, von Wichtigkeit. Er dient dem Schutz eines Objektes durch Maßnahmen in dessen Umfeld bzw. in dem umgebenden freien Raum, in der Regel bis einschließlich zur Grundstücksgrenze

13.2 Gebäude, Fenster, Türen

Bereits beim Bau eines „Rechenzentrums“ (häufig in den letzten Jahren auch „Data-Center“ genannt) ist auf die entsprechenden Sicherheitsmaßnahmen zur Abwehr von gezielten Angriffen und Katastrophen durch geeignete bauliche Maßnahmen, Infrastruktur und Leitungsführung Rücksicht zu nehmen. Das Gebäude ist je nach Szenario vor Bombenanschlägen, Flugzeugabstürzen, Erdbeben, Sturmschäden und ähnlichen Gefahren zu schützen. Möglichkeiten, die Sicherheit von Rechenzentren zu erhöhen, bestehen unter anderem in folgenden Maßnahmen:

- Bauen "in die Tiefe": Zahlreiche Rechenzentren befinden sich heute bereits mehrere Stockwerke unter der Erde.
- Räumliche Trennung und getrennte Absicherung der einzelnen Funktionsbereiche.
- Absicherung von Klima- und Versorgungsschächten gegen mögliche Terroranschläge; Perimeterschutz.
- Verzicht auf Fenster oder Einsatz von Spezialverglasung gegen Durchwurf und Durchbruch, Einsatz innenseitiger Schutzfolie gegen Glassplitter.

Türen, Fenster, Lichtschächte, Dachfenster – in dieser Reihenfolge würde ein geständnisfreudiger Einbrecher wohl seine Vorlieben nennen. Nur wenige Sekunden, ein minimaler Kraftaufwand, vielleicht nur ein Schraubendreher als Werkzeug, und die meisten dieser scheinbaren Hindernisse sind geöffnet.

Schwachstelle Nummer eins in Fragen der Sicherheit sind Fenster und Türen – aber auch die Unbedarftheit der Mitarbeiter: Gekippte oder ungesicherte Fenster sind quasi eine Einladung zum Einstieg, normalerweise sind Rollläden kein großes Hindernis, viele Türen werden ohnehin nicht geschlossen. Hundertprozentig lässt sich keine Tür und kein Fenster sichern, aber zumindest

lassen sich Einstiege so erschweren, dass die meisten der ungebetenen Besucher aufgeben.

Für einbruchhemmende Fenster ist als Standard die DIN V EN 1627 relevant: Ein einbruchhemmendes Fenster ist ein Fenster, das in geschlossenem, verriegeltem und abgeschlossenen Zustand Einbruchsversuche mit körperlicher Gewalt für eine bestimmte Zeit (Widerstandszeit) erschwert.

Aber diese Widerstandszeit muss je nach Wertobjekt unterschiedlich groß sein: Ein Arbeitszimmer verlangt einen anderen Sicherheitsfaktor als ein Serverraum. Die Norm unterscheidet deshalb insgesamt zwischen sechs Stufen von Widerstandsklassen (WK 1 bis WK6): Die Widerstandsklasse WK 1 wird nur dort empfohlen, wo kein direkter Zugang zum Schutzobjekt möglich ist. Für Wohnobjekte sind die Widerstandsklassen WK 2 und WK 3 ausreichend, für normale Büroräume die Widerstandsklasse WK 3. Die Widerstandsklassen ab WK 4 sind für hohe und höchste Gefährdungen vorgesehen. Entscheidend für die Sicherheit ist neben einer soliden Konstruktion und hochwertigen Materialien auch die richtige Montage. Das sicherste Fenster nützt nichts, wenn es falsch montiert wurde.

Für einbruchhemmende Türen kann man ebenfalls auf die DIN V EN 1627 als Sicherheitsstandard zurückgreifen. Es gelten analoge Widerstandsklassen. Der Sicherheitswert einer Tür hängt im wesentlichen vom verwendeten Material für Türblatt und Rahmen (Zarge) sowie von der Rahmenbefestigung, den Bändern (Scharnieren) und den Beschlägen ab. Die Zargen sollten entsprechend solide verarbeitet und fachgerecht in den Wänden verankert sein. Um Einbrecher erfolgreich abzuwehren sind zudem stabile Türbänder und Beschläge erforderlich, die ausreißsicher an Türblatt und Zarge befestigt sind. Der Schließzylinder darf an der Außenseite der Tür nicht überstehen und sollte gegen einfaches Aufbohren geschützt sein.

13.3 Verkabelung

Eine sichere Verkablung zu Kommunikationszwecken hat sich an der DIN EN 50173 zu orientieren. Netzwerkkabel, aktive Komponenten und auch die Netzwerkkarte für das externe Netz sind sehr verletzliche Punkte in einem Netzwerk. Ein Angreifer, der sich unbemerkt an ein Netzwerk anschließen kann, hat es leicht, den Datenverkehr abzuhören und Angriffe auf die für ihn erreichbaren Netzwerke zu starten.

Patch-Panels, Hubs und Switches sollten deshalb in abgeschlossenen Schränken installiert sein, die durch die Alarmanlage des Gebäudes gesichert sind. Kabel sind in Wänden und Decken so zu verlegen, dass ein Anzapfen der Leitung möglichst erschwert wird. Weiter darf der freie Zugriff auf etwaige externe Datenanschlüsse nicht möglich sein.

13.4 Drahtlose Netzwerke

Besondere Beachtung ist dem Einsatz von drahtlosen Netzwerken innerhalb des Rechenzentrums zu schenken. Bei der *drahtgebundenen* Kommunikation wird der Übertragungskanal – in der Regel ein elektrisch leitendes Medium – vom Sender geändert; aus den Änderungen kann der Empfänger die übertragene Information ableiten. Bei der *drahtlosen* Kommunikation ist das Übertragungsmedium die Luft, man spricht bei der Schnittstelle zum Netzwerk auch von der „Luftschnittstelle". Das Übertragungsmedium wird dabei von verschiedenen Systemen gleichzeitig verwendet, so dass der Empfänger genau einen Sender selektieren muss. Dieses gelingt je nach den eingesetzten Systemen und dem betriebenen Aufwand mehr oder weniger gut.

Ohne Sie jetzt mit technischen Details langweilen zu wollen: In dieser „Selektierung" liegt eines der Probleme bei Luftschnittstellen, es kann zu Interferenzen (Überlagerungen) mehrerer Systeme mit Übertragungsstörungen kommen.

Abhörsicherheit

Das zweite Problem liegt in der Abhörsicherheit. Es ist nicht ganz einfach, ein drahtgebundenes Netz unbemerkt anzuzapfen, bei Glasfaserverbindungen ist es sogar recht schwierig. Eine Funkverbindung abzuhören und aktiv mitzuwirken – zu senden, unter falschem Namen etwa – ist dagegen ein Kinderspiel.

Es ist bei Funkverbindungen grundlegend davon auszugehen, dass ein Unberechtigter mithört und als Sender falsche Identitäten benutzt werden. Deshalb dürfen ohne Schutzmaßnahmen wie Verschlüsselung und / oder Steganografie[53] und sicherer Authentifizierung der Kommunikationspartner keine vertraulichen Nachrichten ausgetauscht werden.

Aktuell kommen folgende Funknetze zum Einsatz:

– im Nahbereich bis zu 10 m bei Bluetooth, ZigBee,

---

53 Verstecken einer Nachricht in sinnvollen anderen Daten (z. B. Images).

- im lokalen Bereich innerhalb von Gebäuden z. B. bei WLAN (IEEE 802.11),
- innerhalb begrenzter Zellen für die mobile Kommunikation z. B. beim GSM oder UMTS,
- im Ortsbereich z. B. bei Laser-Richtfunkstrecken oder Ortsfunknetzen,
- im Fernbereich z. B. bei Richtfunkstrecken,
- zur Satellitenübertragung.

Wir wollen uns im Weiteren auf die Betrachtung des Wireless LAN beschränken.

802.11x WLAN (Wireless LAN)

Der Standard IEEE 802.11 wurde für begrenzte Bereiche wie Haushalt, Bürogebäude, Firmenkomplex oder Universitätscampus ausgelegt. Zusätzlich wurden weitere Leistungsmerkmale wie fristenbasierte Dienste, Leistungsmanagement und Sicherheitsmechanismen vorgesehen.

Ein Wireless LAN ist ein lokales Netzwerk, bei dem statt fester Verkabelung mit Verteilern Funkverbindungen genutzt werden. Dazu werden die mobilen Endgeräte mit entsprechenden Adapterkarten ausgerüstet. Wenn zwei mobile Geräte miteinander kommunizieren möchten, reicht es bereits aus, wenn beide mit einer Adapterkarte ausgestattet sind. Soll ein Netz mit mehr als zwei Teilnehmern betrieben werden, benötigt man einen so genannten *Access Point*.

Der Buchstabe hinter der Nummer des Standards, den wir bisher mit dem Platzhalter x belegt haben, bezeichnet die unterschiedlichen Ausprägungen des Standards und kennzeichnet im Wesentlichen die Übertragungsgeschwindigkeit des WLANs.

Wi-Fi

Im Zusammenhang mit konkreten Produkten für 802.11x WLANs taucht häufig der Begriff *Wi-Fi* auf. Was hat es damit auf sich? 1999 wurde ursprünglich unter dem Namen WECA (Wireless Ethernet Compatibility Alliance) eine Vereinigung, bestehend aus einer Vielzahl von Unternehmen, gegründet, die es sich zur Aufgabe gemacht hat, Produkte auf der Basis des IEEE 802.11 Standards zu zertifizieren und somit die Interoperabilität zwischen den Komponenten zu bestätigen. Später benannte sich die WECA in Wi-Fi (Wireless Fidelity) um. Hintergrund war, dass in vielen Produkten der Standard nicht vollständig implementiert bzw. durch proprietäre Erweiterungen aufgeweicht wurde. Somit

ergaben sich häufig Inkompatibilitäten zwischen Produkten verschiedener Hersteller. Wie sieht es nun innerhalb des WLAN-Standards mit der Informationssicherheit aus?

Wired Equivalent Privacy

WEP

Im Standard IEEE 802.11 wird das Sicherheitsprotokoll Wired Equivalent Privacy (WEP) spezifiziert, dessen Implementierung und Benutzung als optional deklariert sind. Das WEP Protokoll soll hauptsächlich drei Ziele erreichen:

Geheimhaltung
Das grundlegende Ziel von WEP ist die Verhinderung eines einfachen Belauschens der über das drahtlose Netz übertragenen Daten.

Zugriffskontrolle
Ein weiteres Ziel ist der Schutz des Zugangs zum drahtlosen Netz. Der Standard IEEE 802.11 definiert zwei Formen der Authentifizierung: *Open System* und *Shared Key*.

Integrität der Daten
Um übertragene Nachrichten vor unbemerkter Veränderung zu bewahren, enthalten mittels WEP verschlüsselte Pakete eine Prüfsumme (Integrity Check Value (ICV)).

Grundlage der WEP-Verschlüsselung ist der Algorithmus Rivest Cipher 4 (RC4) von RSA Data Security, Inc. Er wurde 1987 entwickelt und blieb bis 1994 geheim, bis der Quellcode anonym veröffentlicht wurde. Bei dem von RC4 erzeugten Schlüsselstrom handelt es sich um einen Strom aus pseudo-zufälligen Bytes. Der als Eingabe verwendete Schlüssel hat eine variable Länge und kann bei WEP 40 oder 104 Bit lang sein. Die Verschlüsselung der zu sendenden Daten wird durch eine Verknüpfung der Daten mit dem von RC4 erzeugten Schlüsselstroms erreicht. WEP unterstützt die Verwendung von bis zu vier voreingestellten Schlüsseln, die von Hand in die mobilen Endgeräte und den Access Point eingetragen werden müssen.

Ein Problem von WLANs, welches zunehmend an Bedeutung gewinnt, sind die vorgegebenen Standardeinstellungen. Da die Verbreitung von drahtlosen Netzen ansteigt und die Installation der Geräte immer häufiger durch wenig versierte Benutzer erfolgt, findet die Inbetriebnahme mehr und mehr mit den vorgegebenen Einstellungen statt. Diese werden auch später nur selten verändert, da die Funktionsfähigkeit gegeben und ein ausreichendes Bewusstsein für Sicherheitsaspekte nicht vorhanden ist.

Aufgrund dieser Tatsache ist ein großer Anteil an drahtlosen Netzen komplett ungeschützt. Der Anteil der Netzwerke ohne WEP beläuft sich den aktuellen Statistiken nach auf ungefähr ein Drittel aller installierten WLAN.

Beacon, SSID

Weiterhin wird von einem Access Point in regelmäßigen Abständen ein „Leuchtfeuer“ (Beacon) verschickt, um seine Präsenz anzuzeigen. Der Standard IEEE 802.11 schreibt vor, dass dieses Beacon auch die SSID enthalten muss. Außerdem reagiert ein Access Point normalerweise auf eine Sondierungsanfrage (Probe Request) nach allen Netzen in der Umgebung (SSID "any"). Durch diese beiden Verhaltensweisen ist es leicht, ein drahtloses Netzwerk aufzuspüren. Entsprechende Anleitungen und Software-Scanner wie Kismet, Netstumbler, Airsnort, etc. sind im Internet leicht zu finden.

Aber auch mit aktiviertem WEP ist es leicht möglich, in ein WLAN einzubrechen. Ohne Sie mit Mathematik langweilen zu wollen: Die Sicherheitslücken liegen in der Verwendung der maximal vier *statischen* Schlüssel begründet, die bei jeder Übertragung verwendet werden.

Wi-Fi Protected Access

WPA

Wi-Fi Protected Access (WPA) ist eine weitere Verschlüsselungsmethode für ein Wireless LAN. Nachdem sich die Wired Equivalent Privacy (WEP) des IEEE-Standards 802.11 als unsicher erwiesen hatte und sich die Verabschiedung des neuen Sicherheitsstandards 802.11i verzögerte, wurde durch die Wi-Fi eine Teilmenge von 802.11i vorweggenommen und unter dem Begriff WPA als Pseudostandard etabliert. WPA bietet zusätzlichen Schutz durch *dynamische* Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet optional die Anmeldung von Nutzern über das Extensible Authentication Protocol (EAP) an.

Die erhöhte Sicherheit gegenüber WEP besteht darin, dass der Schlüssel nur bei der Initialisierung verwendet wird und anschließend ein Session Key, der sich bei jeder Sitzung ändert, zum Einsatz kommt. WPA sieht zwei Möglichkeiten der Schlüsselverwaltung vor:

- Die Zugangskennungen bzw. Schlüssel werden auf einem zentralen Server verwaltet (Managed Key), oder
- Es werden "Pre-Shared Keys" (WPA-PSK) genutzt.

Bei der Pre-Shared Keys Methode melden sich alle Nutzer eines Netzes mit demselben Kennwort an. Falls zu kurze und leicht zu erratende Passwörter verwendet werden, liegt hier ein Angriffspunkt für Hacker. Dies ist jedoch keine Sicherheitslücke des WPA-Standards. In diesem Fall hängt die Sicherheit des Systems von der Qualität des Passworts ab. Seit November 2004 existiert das Programm "WPA Cracker", um genau diese Schwachstelle auszunutzen.

WPA2

Am 3. Februar 2004 kündigte die Wi-Fi Alliance die Erweiterung von WPA zu WPA2 an. WPA2 setzt genau wie 802.11i anstatt der RC4-Verschlüsselung den wesentlich sichereren Advanced Encryption Standard (AES) ein.

13.5 Weitere Infrastrukturprobleme und -maßnahmen

Eine störungsfreie Energiezufuhr ist Grundvoraussetzung für die ordnungsgemäße Funktion jedes IT-Verbunds. Moderne Rechner haben eine Pufferzeit von ca. 10 msec. Länger dauernde Netzausfälle können einen unkontrollierten Ausstieg oder Absturz des Systems herbeiführen.

Weiter können Probleme durch Spannungsschwankungen von mehr als ca. +10% und -15% auftreten. Aus diesem Grund ist zumindest für den Server-Betrieb die Installation einer unterbrechungsfreien Stromversorgung (USV) eine Notwendigkeit.

USV

USV-Anlagen haben zwei Funktionen zu erfüllen. Zum einen müssen sie Spannungsschwankungen und kurzzeitige Ausfälle kompensieren, zum anderen die Energieversorgung bei längeren Ausfällen sicherstellen, so dass begonnene Operationen abgeschlossen und Daten aus dem Hauptspeicher auf den Festspeicher geschrieben werden können. Im Allgemeinen können USV-Anlagen Netzausfälle von ca. 10 – 30 Minuten überbrücken Soll die Stromversorgung für längere Zeit sichergestellt werden, so ist die zusätzliche Installation einer Notstromanlage – etwa eines Dieselaggregates erforderlich. Die Pufferzeit einer USV gibt an, wie lange sie mit voll geladenen Batterien bei voller Ausgangsleistung arbeiten kann. Zu beachten ist, dass die Kapazität einer Batterie im Laufe von 3 bis 5 Jahren auf ca. die Hälfte abnimmt.

Elektrostatische Aufladung

Elektrostatische Aufladungen können Schäden an Bauteilen, Fehler in Programmabläufen oder Datenverluste verursachen. Während die Wahrnehmungsschwelle des Menschen bei einer elektrostatischen Aufladung von etwa 2000 V liegt, können bereits Personen, die eine elektrostatische Aufladung von nur 100 V aufweisen, bei direkter Berührung von ICs (anlässlich Wartung,

Demonstration usw.) elektrische Durchschläge verursachen, die das betroffene Bauelement irreparabel zerstören können. Aus diesem Grund wird für Komponenten, die in ungeschützter Umgebung eingesetzt werden, eine relativ hohe Widerstandsfähigkeit gegen elektrostatische Aufladung gefordert. So müssen beispielsweise Chipkarten laut Normbedingungen (/IS0 7816/) elektrostatische Aufladungen von mindestens 1500 V zerstörungsfrei überstehen, handelsübliche Chipkarten bieten meist höhere Werte.

Zieht man allerdings in Betracht, dass abhängig von Bodenbeschaffenheit und Schuhwerk die elektrostatische Aufladung von gehenden Personen 10 kV und mehr betragen kann, so zeigt sich die Notwendigkeit von Maßnahmen zur Vermeidung und Eliminierung elektrostatischer Aufladungen. Solche Maßnahmen sind etwa die Gewährleistung einer relativen Luftfeuchtigkeit von mindestens 50%, die Verwendung geeigneter Werkstoffe (Bodenbeläge,...), Erdungsmaßnahmen oder der Einsatz von Antistatikmitteln.

Schutz vor HF - Strahlung von außen

Mögliche Ursachen für Störstrahlungen, die die Funktion von IT-Komponenten beeinträchtigen können, sind Radarstrahlung, Rundfunk- und Fernsehsender, Richtfunkanlagen, Hochspannungsleitungen und Maschinen, von denen elektromagnetische Störungen ausgehen können. Geeignete Maßnahmen beinhalten die konsequente Abschirmung der IT-Komponenten.

Brandschutz

Die wesentlichen präventiven Brandschutzmaßnahmen sind bereits bei der Errichtung und Ausstattung des Rechenzentrums zu treffen. So müssen entsprechende Brandabschnitte festgelegt und die IT-Bereiche von angrenzenden Bereichen mittels feuerbeständiger Bauteile abgetrennt werden. Weiterhin ist auf die Verwendung von schwer- oder nicht-entflammbaren Materialien zu achten. Bereits in der Planungsphase von Neu- oder Umbauten von Rechenzentren ist unbedingt auch ein Brandschutzsachverständiger einzubinden.

Im täglichen Betrieb ist dafür Sorge zu tragen, dass leicht-entflammbare Materialien möglichst ausgelagert werden. Die Lagerung großer Papiermengen in Drucker- oder Kopierräumen stellt ebenso ein oft zu wenig beachtetes Risiko dar, ebenso wie die Aufbewahrung großer Mengen von Reinigungsmitteln. Rauchverbote im Rechenzentrum, Aschenbecher am Eingang zu Rauchverbotszonen sowie die Verwendung von selbst löschenden Papierkörben sollten ebenfalls zu den selbstverständlichen Brandverhütungsmaßnahmen gehören.

Branddetektoren, Alarmierungssysteme

Branddetektoren arbeiten auf der Basis von Rauch- und / oder Temperaturerkennung und werden im Allgemeinen mit Alarmierungssystemen und automatischen Löschvorrichtungen kombiniert. Dabei unterscheidet man zwei Grundprinzipien:

Wärmemelder reagieren auf eine Temperaturerhöhung. Maximalmelder sprechen an, wenn die gemessene Kenngröße einen bestimmten Wert für eine genügend lange Zeit überschreitet, Differentialmelder sprechen an, wenn die Änderungsgeschwindigkeit der gemessenen Kenngröße einen bestimmten Wert für eine genügend lange Zeit überschreitet.

Rauchmelder reagieren auf in der Luft enthaltene Verbrennungs- und / oder Pyrolyseprodukte (Schwebstoffe). Ionisationsrauchmelder sprechen auf diejenigen Verbrennungsprodukte an, welche den Ionisationskammerstrom im Melder beeinflussen können. Optische Rauchmelder sprechen auf Verbrennungsprodukte an, welche die Dämpfung oder die Streuung von Licht im infraroten, sichtbaren und / oder ultravioletten Bereich des elektromagnetischen Spektrums beeinflussen können

Geräte und Einrichtungen, die besonders überwacht bzw. gegen Brände geschützt werden müssen, sind CPUs, Plattenspeicher und Kassettenstationen, Netzwerkschränke, Vorrechner und Netzknotenrechner, Drucker und Archive. Auch infrastrukturelle Einrichtungen wie Netzverteiler, Energieversorgung einschließlich USV, Klimaanlage bzw. Klimaschränke, Doppelboden und Zwischendeckenraum müssen in das Schutzkonzept miteinbezogen werden.

Um Brände bereits in der Entstehungsphase schnell und zuverlässig zu entdecken, wird zunehmend neben der Raumüberwachung eine zusätzliche Überwachungsebene direkt am Gerät installiert.

Überspannungsschutz und Blitzschutz

Unter *Überspannungsschutz* versteht man die Summe aller technischen Vorkehrungen, die dazu dienen, Störfaktoren der Stromversorgung auszuschalten, die zu überhöhten Spannungen führen können. Solche Störungen können beispielsweise durch Blitzschlag, mangelhafte Erdung oder eine falsche Verlegung der Datenleitungen hervorgerufen oder über das Versorgungsnetz übertragen werden.

Man unterscheidet zwischen Überspannungsschutzgeräten für den Grob- und solche für den Feinschutz. *Grobschutzanlagen* vermindern Überspannungen auf ein für Starkstromanlagen ungefährliches Niveau. Sie weisen überdies ein hohes Ableitvermö-

gen für den Blitzstrom auf. Für IT-Anlagen ist die Kombination mit *Feinschutzanlagen* erforderlich: Das sind Anlagen, die Überspannungen soweit herabsenken, dass sie auch für Mikroelektronikkomponenten ungefährlich sind. In den Schutz einzubeziehen sind vor allem Rechner, Endgeräte, Übertragungsleitungen, Mess- und Steuereinrichtungen und die Sicherheitselektronik.

Für Gebäude, in denen Rechenzentren oder DV-Komponenten untergebracht sind, sind entsprechende Blitzschutzanlagen vorzusehen.

13.6 Richtlinien zur Zutrittskontrolle

Essentiell gerade im Hinblick auf etwaige Zertifizierungen nach dem ISO 27001 oder dem Grundschutzhandbuch ist, wie bereits eingangs erwähnt, die generelle

Festlegung der Zutrittskontrollpolitik:

Im Sicherheitskonzept wird festgelegt, welche Personengruppen (etwa Operator, RZ-Mitarbeiter, Fachabteilungsmitarbeiter, Kunden, Angehörige von Lieferfirmen etc.). Zutritt zu welchen Bereichen benötigen.

Definition eines Verantwortlichen:

Dieser vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den Vorgaben des Sicherheitskonzeptes.

Definition von Zeitabhängigkeiten:

Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit, Zutritt einmal täglich oder befristeter Zutritt bis zu einem fixierten Datum.

Festlegung der Zutrittskontrollmedien:

Es ist festzulegen, ob die Identifikation bzw. die Authentisierung durch Überwachungspersonal (persönlich oder über TV-Kontrollen) oder durch automatische Identifikations- und Authentisierungssysteme wie Karten oder biometrische Methoden erfolgen soll.

Festlegung der Beweissicherung:

Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden sollen (mitbestimmungspflichtig!). Weiter sind folgende Fragen zu klären:

- Sind beim Betreten und / oder Verlassen eines geschützten Bereiches Vereinzelungsmechanismen (Drehtüren, Schleusen, ...) notwendig?
- Ist das Auslösen eines "stillen Alarms" vorzusehen? Durch Eingabe einer vereinbarten Kennung, etwa einer zusätzlichen Ziffer zur üblichen PIN, wird ein Alarm an einer entfernten Überwachungsstelle (Pförtner, Polizei) ausgelöst. Eine solche Maßnahme bietet Schutz gegen jemanden, der den Zugang zu geschützten Bereichen gewaltsam erzwingen will.

Bei automatischer Personenidentifikation sind zudem die Gültigkeitsdauer für die Zutrittskontrollmedien (Schlüssel, Codes, etc.) festzusetzen sowie die Sperrmöglichkeiten bei Verlust oder Duplizierung des Schlüssels und bei Austritt eines Mitarbeiters zu prüfen.

Die Zutrittskontrollpolitik sollte bereits vor der Systemauswahl so detailliert wie möglich feststehen und weitgehend stabil bleiben. Überarbeitungen werden jedoch notwendig, wenn Sicherheitsmängel festgestellt werden, bei schlechter Benutzerakzeptanz, deren Ursache etwa zu lange Wartezeiten oder psychologische Faktoren (z. B. bei biometrischen Systemen) sein können, sowie bei einer Erweiterung des sicherheitsrelevanten Bereiches.

Rechteverwaltung

Für die Rechteverwaltung im Bereich Zutrittskontrolle gelten ähnliche Vorgaben und Regeln wie im Bereich der Zugangs- und Zugriffskontrolle. Die Subjekte sind hier generell Personen, die Objekte Räume, Gebäude oder Geräte. Im Allgemeinen besteht nur eine Art von Rechtebeziehung, nämlich "ein Subjekt S *hat Zutritt zu* einem Objekt O". Allerdings sind Zutrittsberechtigungen im Allgemeinen sehr viel stärker an zeitliche Einschränkungen gebunden als Rechte im Bereich der Zugriffskontrolle.

Nullsummenprüfung

Hierbei handelt es sich um die Feststellung der Anzahl der im geschützten Bereich befindlichen Personen durch Vergleich der Zu- und Abgänge. Voraussetzung für eine Nullsummenprüfung ist die Installation von Vereinzelungsmechanismen.

13.7 Verfahren der Zutrittskontrolle

Die Identifikation bzw. Authentisierung einer Person durch eines oder mehrere der drei Grundprinzipien Wissen, Besitz oder persönliche Eigenschaften (charakteristisches Merkmal) ist im Be-

reich Zutrittskontrolle deutlich anders ausgeprägt als bei der Rechnerzugangs- oder -zugriffskontrolle.

Authentisierung durch Wissen

Für die Zutrittskontrolle werden im Allgemeinen Codes eingesetzt, die an einer neben der Tür angebrachten Tastatur einzugeben sind. Da diese Codes üblicherweise nicht personenbezogen, sondern geräte- oder firmenspezifisch sind (eine Person wird also nicht als Individuum authentisiert, sondern lediglich als Angehöriger einer bestimmten Gruppe), ist das Bedrohungspotenzial bei einer unbefugten Weitergabe sehr hoch. Solche Codes müssen daher zumindest in regelmäßigen, nicht zu großen Zeitabständen geändert werden.

Authentisierung durch Besitz

Diese Verfahren spielen in der heutigen Praxis – manchmal in Kombination mit biometrischen oder wissensbasierten Methoden – die wichtigste Rolle bei Zutrittskontrollsystemen. Alle Arten von Kartentechnologien – ob Magnet-, Induktiv- oder Chipkarten – werden ebenso eingesetzt wie Erkennungsmarken und, in etwas weiterem Sinne, herkömmliche Schlüssel.

Neue Entwicklungen weisen in Richtung der RFID-Technologie (Radio Frequency Identity Tags). Dabei werden kleine Transponder in Stecknadelkopfgröße unter die Haut des Zugangsberechtigten implantiert und von Scannern an den kontrollierten Türen ausgelesen. Implantierte RFIDs verbinden die Authentisierungsmöglichkeiten durch Besitz mit biometrischen Verfahren.

Authentisierung durch biometrische Verfahren

Biometrische Verfahren eignen sich von ihrer Natur her sehr gut für Zutrittskontrollsysteme. Die Unmöglichkeit, biometrische Parameter zu vergessen oder weiterzugeben, ist insbesondere für die Überwachung des physischen Zutritts von Vorteil. Dennoch sind derartige Verfahren in der Praxis heute noch vorwiegend auf den Schutz von Hochsicherheitsbereichen beschränkt. Die Erfahrung zeigt, dass Akzeptanzprobleme, der hohe technische Aufwand und die relativ langen Prüfzeiten einen sehr zögernden Einsatz biometrischer Verfahren in betrieblichen Anwendungen zur Folge haben.

Rechteprüfung

Im Sicherheitskonzept ist festzulegen, wo, zu welchen Zeiten und unter welchen Randbedingungen eine Rechteprüfung erfolgen muss, sowie die Aktionen, die bei versuchtem unerlaubten Zutritt in Kraft treten. Ebenso ist die Behandlung von Ausnahmesituationen zu planen. Beispielsweise ist unter anderem sicherzustellen, dass im Brandfall die Mitarbeiter schnellstmöglich die gefährdeten Zonen verlassen können.

Beweissicherung

Innerhalb dieses Themas sind die folgenden Fragen zu beantworten:

- Welche Daten sollen bei Zutritt zu bzw. Verlassen von Sicherheitszonen protokolliert werden?
- Wo werden diese Informationen aufgezeichnet?
- Wer darf unter welchen Umständen auf diese Informationen zugreifen und nach welchen Kriterien die Daten auswerten?

Bei der Diskussion dieser Fragen ist meist die Mitarbeitervertretung zu beteiligen.

Die hier vorgestellten Maßnahmen sind nicht nur aus rein technischer Sicht zu beurteilen. Vielmehr bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre des Einzelnen. Weiterhin ist zu berücksichtigen, dass die Protokollierung personenbezogener Daten der Zustimmungspflicht des Betriebsrates unterliegt.

Rahmenbedingungen

Die bisher behandelten Fragestellungen beziehen sich auf die *Sicherheit* von Zutrittskontrollsystemen. Für den Einsatz in der betrieblichen Praxis sind jedoch eine Reihe weiterer Kriterien von Bedeutung. So müssen die Kosten für die Installation, den laufenden Betrieb, die Wartung und die regelmäßige Revision des Zutrittskontrollsystems in vertretbarer Relation zum möglichen Sicherheitsrisiko stehen. Die Kapazität des Zutrittskontrollsystems muss der Firmengröße und -organisation angepasst sein. Insbesondere ist eine ausreichende Zahl von Kontrollstellen und eventuellen Vereinzelungsmechanismen vorzusehen, um Warteschlangen auch zu Stoßzeiten zu vermeiden.

Zutrittskontrollen werden von den meisten Menschen als notwendiges Übel betrachtet. Bei mangelnder Akzeptanz steigt die Gefahr, dass das System entweder generell abgelehnt wird, oder aber, dass die Mitarbeiter versuchen, das System nach Möglichkeit auszuschalten. Zu solchen Umgehungsmaßnahmen zählen etwa das Offenhalten von Türen oder die unbefugte Weitergabe von Zutrittskontrollmedien.

Es sind daher alle Maßnahmen zu treffen, um die Akzeptanz von Zutrittskontrollsystemen so hoch wie möglich zu gestalten. Möglichkeiten dazu sind kurze Antwortzeiten, eine einfache Bedienung und gute Bedienerführung sowie der Verzicht auf Authentisierungssysteme, gegen die psychologische Barrieren zu erwarten sind. Ganz besonders wichtig ist die Sicherstellung der

Transparenz für den Benutzer, insbesondere offene Information darüber, welche Daten wie lange gespeichert und wie sie verarbeitet werden.

14 Sicherheitsmanagement – die tägliche Praxis

Nach den vorbereitenden und konzeptionellen Arbeiten sowie den PDCA-Tätigkeiten, die wir im Abschnitt 2.2 betrachtet haben, behandeln wir jetzt die Tätigkeiten, die nach Umsetzung aller Maßnahmen des Sicherheitskonzeptes zur täglichen Praxis des Sicherheitsmanagements gehören.

14.1 Aufrechterhaltung der Sicherheit

Hinter diesem Titel verbergen sich alle Aktivitäten, mit denen das Sicherheitsmanagement überprüft, ob die Sicherheit so gelebt wird, wie es in der Sicherheitsleitlinie und im Sicherheitskonzept (und den mitgeltenden Dokumenten) geplant worden ist. Dazu sind folgende Aktivitäten geeignet:

- Gespräche mit Mitarbeitern führen, dabei über Erfahrungen mit der Sicherheit berichten lassen,
- das Vorhandensein von wichtigen Sicherheitsdokumenten am Arbeitsplatz prüfen,
- Regeln und andere Vorgaben stichprobenartig auf Einhaltung prüfen,
- Konfigurationen technischer Systeme mit den Vorgaben abgleichen,
- die aktuellen Firewall-Regeln mit der Vorgabe angleichen,
- technische Untersuchungen, z. B. Penetrationstests durchführen (lassen),
- Kontrolle ausgefüllter Checklisten,
- Prüfen von Log-Protokollen und anderen maschinellen Aufzeichnungen.

Solche Aktivitäten sollten Sie planen, um über das Jahr verteilt genügend Zeit zu haben, alle Punkte sorgfältig abarbeiten zu können. Über jede ausgeführte Aktivität legen Sie Aufzeichnungen an. Diese bilden dann einen wesentlichen Input für die Phase *check* im PDCA-Zyklus.

Gibt es einen Anlass, das Sicherheitsverhalten eines Mitarbeiters kritisch zu hinterfragen oder eine intensive Prüfung eines Ar-

beitsplatzes vorzunehmen, sollten Sie die Personalvertretung vorab informieren und mit einbeziehen.

14.2 Management von Sicherheitsvorfällen

Natürlich hat man die Absicht, Sicherheitsvorfälle gar nicht erst entstehen zu lassen. Dennoch zeigt die Erfahrung auch bei perfekt geplanter Sicherheit: Der nächste Sicherheitsvorfall kommt bestimmt! Sicherheitsvorfälle kann man einteilen in „Notfälle“ und andere (nicht so gravierende) Vorfälle:

- Als Notfall gilt jeder eingetretene Vorfall, der eine nicht tolerierbare Beeinträchtigung von Sicherheitszielen oder einen für das Unternehmen gravierenden Schaden mit sich bringt.
- Bei den „anderen Vorfällen“ geht es um solche, bei denen die Beeinträchtigung von Sicherheitszielen temporär toleriert werden kann und die insgesamt vom Schaden her nicht gravierend sind.

Eine andere Unterteilung ergibt sich aus folgendem Sachverhalt: Es gibt Sicherheitsvorfälle,

- die man beim Sicherheitskonzept schon als Bedrohung berücksichtigt hat (Klasse A), und
- solche, die man nicht berücksichtigen konnte, weil die Art des Vorfalls unbekannt war oder weil man schlicht etwas übersehen hat (Klasse B).

Für Vorfälle der Klasse B besteht das Problem darin, dass man quasi unvorbereitet getroffen wird und unklar ist, welche Auswirkungen der Vorfall haben kann.

Es wird vorkommen, dass Vorfälle der Klasse A nicht ausreichend durch Maßnahmen abgefangen werden können, ihr Eintreten aber einen exorbitanten Schaden nach sich zieht. Solche Fälle der Klasse A und generell alle Fälle der Klasse B stellen *Notfälle* dar.

Notfallhandbuch

Für Notfälle muss man sich einen Plan zurechtlegen, wie man bei ihrem Eintreten vorgeht. Genau dies ist der Inhalt des so genannten *Notfallhandbuchs*: Es soll eine praktikable Handlungsanleitung geben, um den jeweiligen *Schaden* zu begrenzen und das weitere Management des Vorfalls zu ermöglichen – verhin-

dern[54] kann man ihn nicht mehr, denn er ist ja bereits eingetreten.

Management

Für das Management von Sicherheitsvorfällen kommt es generell darauf an,

- zunächst einen sicheren Meldeweg zu etablieren, auf dem ein vermeintlicher oder tatsächlicher Sicherheitsvorfall das Sicherheitsmanagement erreicht,
- den Vorfall zu dokumentieren und in seiner Wichtigkeit zu klassifizieren,
- bei Notfällen zunächst den Schaden zu begrenzen (wie zuvor erläutert),
- den Vorfall systematisch zu analysieren und – wenn möglich – korrektive und vorbeugende Maßnahmen vorzusehen, um weitere Fälle dieser Art auszuschließen oder ihre Auswirkung zu begrenzen,
- zu prüfen, ob es Rückwirkungen auf das Sicherheitskonzept (z. B. notwendige Anpassungen bei den Analysen und Maßnahmen) oder vielleicht sogar auf die Sicherheitsleitlinie gibt (s. Abschnitt „2.2 Das PDCA-Modell“),
- mindestens bei Notfällen der Unternehmensleitung einen zusammenfassenden Bericht zu geben (s. Abschnitt „14.3 Berichtswesen“).

Meldeweg

Jeder Mitarbeiter muss über die Information verfügen, an wen er sich bei einem Sicherheitsvorfall wenden muss. Es ist nicht sinnvoll, diese Information nur elektronisch (z. B. im Intranet) vorzuhalten – bei einem Sicherheitsvorfall kann diese Information nicht mehr zugänglich sein.

Je nach Größe des Unternehmens kann es erforderlich sein, Meldungen über Vorfälle zunächst „vorfiltern“ zu lassen, um die Spreu vom Weizen zu trennen. Hier könnte beispielsweise ein User Help Desk sehr hilfreich sein, das erst bei Sicherheitsvorfällen im engeren Sinne eine Meldung an das Sicherheitsmanagement weiterreicht.

---

[54] Alles was zur *Verhinderung* von Sicherheitsvorfällen vorgesehen ist, ist Bestandteil des Sicherheitskonzeptes und hat im Notfallhandbuch nichts zu suchen!

Klassifizierung

Zur Klassifizierung von Sicherheitsvorfällen sollte man sich ein Schema mit 3 – 5 Stufen vorgeben, die die Wichtigkeit eines Vorfalls charakterisieren und die angemessene Reaktion festlegen. In der Tabelle 17 ist ein *vereinfachtes* Beispiel mit 3 Stufen dargestellt:

Tabelle 17: Klassifikationsschema für Sicherheitsvorfälle

Nr.	Klasse	Reaktion	Reaktionszeit
1	informativ	zur Kenntnis nehmen, für eine spätere Bearbeitung vorsehen	hat Zeit
2	erheblich	der Angelegenheit nachgehen, Analyse, Behebung / Korrektur	gleich
3	Notfall	Schaden begrenzen, vorläufige Behebung, Analyse, systematische Behebung / Korrektur	sofort

Es gilt die folgende Regel: Ist nicht eindeutig festzustellen, um welche Klasse von Vorfall es sich handelt, stuft man den Vorfall grundsätzlich als „Notfall“ ein.

Unsere Checkliste, die bei jeder Meldung auszufüllen ist, muss eine Spalte enthalten, in der die Klassifikation des Vorfalls eingetragen wird.

Dieses Beispiel mit 3 Klassen hat den Nachteil, dass man „instinktiv“ meist in die Mitte – Klasse 2 – geht. Deshalb ein Tipp: Nehmen Sie für die Praxis eine *gerade* Zahl (4 oder 6) von Klassen.

Analyse

Bei der Analyse geht es zunächst darum, den Vorfall, seine Ursachen und Auswirkungen genau zu verstehen. Aufzeichnungen der Systeme oder von Verantwortlichen bei manuellen Vorgängen können hierbei helfen. Danach ist zu prüfen, ob dieser Vorfall im Sicherheitskonzept als Bedrohung aufgeführt ist. Wenn ja, liegt offensichtlich ein Problem mit der dazu gehörenden Maßnahme vor. Wurde eine solche Bedrohung nicht im Sicherheitskonzept betrachtet, muss diese nachträglich eingefügt und eine entsprechende Korrekturmaßnahme in Betracht gezogen werden.

Arbeitsanweisung

Für die Behandlung von Sicherheitsvorfällen (gleich welcher Klasse) brauchen wir eine Planung – andernfalls würden wir ja „planlos“ vorgehen, was absolut kontraproduktiv ist. Diesen „Plan“ gießen wir in eine Arbeitsanweisung für das Sicherheits-

management. Titel: „Behandlung von Sicherheitsvorfällen“. In dieser Arbeitsanweisung wird für Notfälle auf das Notfallhandbuch verwiesen. Die Arbeitsanweisung ist durch eine Checkliste zu ergänzen, die bei jedem Sicherheitsvorfall ausgefüllt wird und zur Analyse und Dokumentation des Vorfalls dient.

Damit weist das Sicherheitsmanagement nach, welche Sicherheitsvorfälle eingetreten sind, wie sie behandelt und welche Schlussfolgerungen daraus gezogen wurden. Diese Informationen tragen auch zu den Phasen *check* und *act* im PDCA-Modell bei.

14.3 Berichtswesen

Das Sicherheitsmanagement wird meist durch die Unternehmensleitung verpflichtet, eine Reihe von Berichten zu liefern. Standardmäßig sollte berichtet werden über

- die Abarbeitung des PDCA-Zyklus durch das Sicherheitsmanagement (s. Abschnitt 2.2),
- gravierende Sicherheitsvorfälle und ihre Folgen (s. Abschnitt 14.2),
- die Ergebnisse interner und externer Audits.

Meist wird auch ein jährlicher Bericht zur Lage der Unternehmenssicherheit gefordert, zu dem das IT-Sicherheitsmanagement Beiträge liefert.

Wichtig ist, dass sich das Sicherheitsmanagement nicht selbst in eine Stress-Situation bringt und nur noch dazu kommt, Berichte zu schreiben und andere wichtige Tätigkeiten vernachlässigt. Insofern sei angeraten,

- für die üblichen Berichte „gute“ Dokumentvorlagen verfügbar zu haben,
- die Standard-Berichte terminlich gut zu planen und über das Jahr zu verteilen,
- einen ersten Entwurf z. B. des Jahresberichtes aus den gespeicherten Aufzeichnungen quasi zu generieren.

Wenn man alle Hinweise zum Thema „Aufzeichnungen“ und „Nachweise“ in diesem Buch beachtet hat, stellt man fest, dass man eine Vielzahl von Informationen sammelt und im Grunde jederzeit jeden gewünschten Nachweis von Sicherheit, Aufgabenerledigung und Ordnungsmäßigkeit erbringen kann. Wichtig

ist auch hier, diese Informationen geeignet zu speichern bzw. abzulegen, wozu eine entsprechende Vorplanung gehört.

15 IT Compliance

15.1 Unternehmensstrategie

Jede Institution, die die Dienste einer IT-Infrastruktur für die Erfüllung ihrer Geschäftsprozesse in Anspruch nimmt, verfolgt in längerfristigen Planungen und Aktivitäten die Realisierung der Vision einer für ihre Belange optimalen IT.

IT-Strategie

Diese Planungen und Aktivitäten – auch als IT-Strategie bezeichnet – leiten sich grundsätzlich aus der bestehenden Geschäftsstrategie ab und lassen sich wie folgt gliedern:

- Die IT-Strategie *berücksichtigt* einerseits *Geschäftswachstumschancen* zur Umsatz- und Ertragssteigerung eines Unternehmens.
- Andererseits enthält die IT-Strategie grundlegende *Anforderungen aus dem Geschäftsbetrieb,* nämlich die *Geschäftsprozesse* mittels Einsatz von IT effizienter zu gestalten und an den zu beachtenden und zu befolgenden Regularien und Gesetzen auszurichten.

Eine IT-Strategie besteht im Wesentlichen aus fünf Komponenten:

- Die *Infrastrukturstrategie* betrachtet die drei IT-Basistechnologien: Hardware, Betriebssysteme und Netzwerke. Ziel der Infrastrukturstrategie ist es, mit möglichst geringen Kosten eine hohe Rechenleistung, Performance und Bandbreite in einem Unternehmen zur Verfügung zu stellen.
- Die *Applikationsstrategie* befasst sich mit dem Einsatz von Software zur Unterstützung von Geschäftsprozessen. Mit der Applikationsstrategie können zwei Ziele verfolgt werden: Einerseits der Einsatz von Software zur Ertragssteigerung, andererseits Software zum effizienteren Geschäftsbetrieb.
- Die *Innovationsstrategie* beschäftigt sich mit IT-Innovationen. Ziel der Innovationsstrategie ist es, neue Technologien vorausschauend für den Einsatz in einem Unternehmen zu bewerten.

- Die *Sourcingstrategie* setzt sich mit der IT-Wertschöpfungskette in einem Unternehmen auseinander. Ziel der Sourcingstrategie ist es, festzulegen, welche IT-Leistungen durch das Unternehmen selbst erstellt und welche eingekauft werden.
- Die *Qualitätssicherungsstrategie* betrachtet die Entscheidungen zur Qualitätssicherung in der IT eines Unternehmens, abgeleitet aus den Einzelstrategien Infrastrukturstrategie, Applikationsstrategie, Innovationsstrategie und Sourcingstrategie. Ziel ist es, die Vorgehensweise festzulegen, mit der vorgegebene Ziele möglichst effizient erfüllt werden können.

Wie wir gleich sehen werden, ist die so genannte *Compliance* ein wesentlicher Bestandteil der Qualitätssicherungsstrategie. Die wirtschaftlich sinnvolle Erfüllung der Compliance ist in der Regel komplex und erfordert eine sorgfältige Planung.

Bei vielen Aspekten der Compliance sind eine realistische, nachvollziehbare Einschätzung der IT-Risiken innerhalb des betrachteten Bereiches und ein adäquater Umgang mit ihnen gefordert.

In diesem Kapitel wollen wir den Zusammenhang der IT-Strategie und der IT-Risikomanagement-Strategie aufzeigen und die wichtigsten Details vertiefen.

15.2 Compliance als essentieller Bestandteil der IT-Strategie

Compliance bedeutet in unserem Kontext die nachweisliche Einhaltung von Regeln und gesetzlichen Vorschriften durch das Management. Neben der Gesetzeskonformität handelt es sich hierbei um die Einhaltung guter Grundsätze zur Unternehmensführung durch die Schaffung adäquater Rahmenbedingungen für bestmögliche Managemententscheidungen sowie die lückenlose Dokumentation der Geschäftsabläufe in Verbindung mit dem Hard- und Software-Einsatz.

Welche Gesetze und Regelungen sind wesentlich für die Compliance?

SOX

Zurzeit weitet sich auch die europäische Gesetzgebung zur Regelung der Unternehmensberichterstellung aus. Die Europäische Union plant in Anlehnung an SOX (Sarbanes-Oxley Act) eine Bilanzabschlussprüfrichtlinie (8. EU Richtlinie), in der viel detaillierter als bisher festgelegte Verhaltensregeln in Verbindung mit dem IT -Einsatz auf Einhaltung überprüft werden müssen.

Sarbanes-Oxley Act ist ein US-Gesetz zur Regelung der Unternehmensberichterstattung, welches als Reaktion auf eine Folge von Bilanzskandalen von Unternehmen wie Enron oder Worldcom erlassen wurde und von jedem an der NYSE (New York Stock Exchange) gehandelten Unternehmen, gleich welcher Nationalität, zu befolgen ist.

Ziel dieses Gesetzes ist, das Vertrauen der Anleger in die Richtigkeit der veröffentlichten Bilanzdaten von Unternehmen wiederherzustellen.

Aus diesem Grund müssen in der Section 302 von SOX die Entscheidungsträger des berichterstattenden Unternehmens mit ihrer Unterschrift versichern, dass "...keine unwahren und irreführenden Informationen in dem Abschluss enthalten sind, Kontrollen zum Schutz vor diesen Falschaussagen implementiert sind und sie sich von der Wirksamkeit dieser Kontrollen persönlich überzeugt haben...".

Die Section 404 von SOX sieht die Einrichtung eines funktionsfähigen internen Kontrollsystems und dessen Dokumentation vor. Dies gilt für alle internen Kontrollen, die im Zusammenhang mit der Rechnungslegung stehen. Der Dokumentation dieses internen Kontrollsystems kommt eine erhebliche Bedeutung zu.

ITIL

In diesem Zusammenhang ist auch /ITIL/ eine wichtige Vorgabe, die herstellerunabhängig detaillierte Richtlinien und Verfahren von IT-Serviceleistungen beschreibt und einen Standard beispielsweise für die Einhaltung von Service Level Management (SLM) und hoher Qualität vorgibt.

Identitäts-management

Weiter ist aus rechtlicher Sicht über den gesamten Lebenszyklus bei den bilanzrelevanten IT-Infrastrukturen und Applikationen die Integrität und Nachvollziehbarkeit lückenlos nachzuweisen. Eine Vielzahl von Vorschriften sowie Anweisungen aus dem Datenschutz-, Arbeits- und Telekommunikationsrecht und auch Vereinbarungen mit Unternehmenspartnern sind zu beachten. Sämtliche Anwendungen müssen durch Identitätsmanagement geschützt werden.

Identitätsmanagement hat zum Ziel, die Identität eines Benutzers zweifelsfrei nachzuweisen, egal wo der Benutzer sich befindet, was er tut und mit welchem Endgerät er Zugang zur IT-Infrastruktur des Unternehmens erhält.

Weiterhin müssen die Unternehmen belegen können, wie sie ihre IT-Sicherheit in Bezug auf Datenschutz, Zugriffskontrollen und Benutzerverwaltung durchsetzen oder die Auswirkungen

von Ereignissen – beispielsweise gravierende technische Störungen – auf ihre Geschäftsprozesse verhindern.

Was häufig übersehen wird: Auch das Management von Software-Lizenzen und die Beachtung von Copyright-Bestimmungen gehört zur Compliance eines Unternehmens!

Je stärker ein Unternehmen von rechnergestützter Informationsverarbeitung abhängig ist, desto wichtiger sind Instrumente zum Schutz vor Datenverlust, Datenkorruption und unerlaubten Datenzugriffen. Zum nachhaltigen Schutz von Daten und Dokumenten jeglicher Art sollten sämtliche Sicherungs-, Controlling- und Initiativmaßnahmen in die Unternehmensorganisation integriert werden.

Neben Sarbanes-Oxley Act (SOX) und der 8. EU-Auditrichtlinie gibt es weitere Regelwerke, die sich auch auf diesen Themenkreis beziehen: das Transparenz- und Publizitätsgesetz (TransPuG), das Aktiengesetz in der Fassung vom 27.04.2001, das Anlagenschutzverbesserungsgesetz (AnSVG) vom 30.10.2004, die Grundsätze zum Datenzugriff und Prüfbarkeit digitaler Unterlagen (GDPdU), die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und das Basel II Rating zur Kreditvergabe.

Sie sehen, es gibt viele Regelungen und Gesetze, deren effiziente Erfüllung unter wirtschaftlichen Aspekten ein wichtiges strategisches Ziel ist. Ein beträchtlicher Schaden kann entstehen, wenn Regelungen und Gesetze nicht eingehalten werden – dazu reicht schon ein mit einer bestimmten Wahrscheinlichkeit eintretendes technisches oder menschliches Versagen. Es entstehen dadurch Risiken im Zusammenhang mit der Compliance, mit denen adäquat umzugehen ist. Diesen Zusammenhang wollen wir uns im nächsten Abschnitt näher ansehen.

15.3 Compliance und Risikomanagement

Wie wir gesehen haben, kann die Nichtbeachtung oder nur teilweise Erfüllung von Compliance-Zielen mit empfindlichen Strafen und indirekten Schäden wie Imageverlust, Wettbewerbsnachteilen, Abwanderung von Kunden etc. behaftet sein.

Nun hat jede IT-Infrastruktur Schwachstellen technischer und organisatorischer Art. Technik ist oft fehleranfällig und unzureichend, Menschen sind keine Automaten und können sich unangemessen und falsch verhalten, was häufig unter dem Begriff „menschlicher Faktor“ zusammengefasst wird.

Nun wissen wir ja bereits, dass ein möglicher, zu erwartender Schaden als Risiko bezeichnet wird. Zu einer sinnvollen IT-Strategie gehört es, diese Risiken im Vorfeld abzuschätzen und den Umgang mit ihnen festzulegen. In der Regel werden Aktionen festgelegt, die zum Ziel haben, das Restrisiko (dazu später mehr), das immer existieren wird, auf einen akzeptablen Wert zu reduzieren.

Welche Aktionen nun genau vorzunehmen sind und wie das Restrisiko definiert ist, wird zuvor in der mit den Unternehmenszielen harmonisierten Risikostrategie festgelegt. Beispielsweise kann es Strategie eines Unternehmens sein, Risiken, die eine Bedrohung der Vertraulichkeit von Informationen beinhalten, besonders stark zu minimieren, während Risiken für die Verfügbarkeit von Teilen der IT-Infrastruktur toleranter behandelt werden. Risikoanalyse, Risikobehandlung und Adaption der Maßnahmen zur Reduzierung des Restrisikos an die sich ständig ändernde IT-Infrastruktur sind die wesentlichen Inhalte des Risikomanagements.

Selbsteinschätzung

Wir haben eine so genannte Selbsteinschätzung (Self-Assessment) der Effektivität unserer Schutzmaßnahmen[55] durchzuführen.

Diese Selbsteinschätzung wird von einigen Gesetzen und Regularien explizit gefordert, beispielsweise vom Sarbanes-Oxley Act und von der ISO 27001[56]. Diese Selbsteinschätzung stellt ein offizielles Statement der Geschäftsleitung dar und wird von Auditoren oder Prüfern auf Vollständigkeit, Korrektheit und Gültigkeit überprüft, bei den Tests festgestellte Abweichungen werden als „issue" dokumentiert. Es wird je nach Größe der Abweichung zwischen kleinen („minor issues") und größeren Abweichungen („major issues") unterschieden. Je nach Gesetz oder Regularium, für das eine Selbsteinschätzung durchgeführt wird, bedeutet eine größere Abweichung (ggf. auch mehrere kleinere Abweichungen) bereits, dass die Compliance nicht mehr gegeben ist.

---

55 Schutz- oder Sicherheitsmaßnahmen werden im Englischen als „Control Measurements" oder auch kurz als „Controls" bezeichnet und sind oft einfach als „Kontrollen" ins Deutsche übernommen worden, was nicht ganz korrekt ist.

56 Dort als Management-Bewertung bezeichnet, die sich u. a. auf interne Audits stützt.

16 Zum Schluss...

Sie haben in diesem Buch eine Reihe vom Methoden und Verfahren sowie Maßnahmen zum Thema Informationssicherheit kennen gelernt. Wie schon im Vorwort gesagt, sind eine begrifflich stabile Grundlage und eine klare Vorgehensweise bei den verschiedenen Analysen unerlässlich für ein gutes Sicherheitskonzept. Bei der Auswahl von Maßnahmen benötigt man zumindest einen Überblick über die verschiedenen Maßnahmenklassen und die Validierung einzelner Maßnahmen.

Wie geht es nun weiter? Was gibt es sonst noch?

Produkteigenschaften

Sicherlich sind Sie für Ihre tägliche Praxis an Aussagen über die Sicherheitseigenschaften konkreter IT-Produkte interessiert. Solche Aussagen haben wir aus nahe liegenden Gründen hier nicht getroffen, sondern verweisen auf Aussagen der Hersteller, bewertende Aussagen in Fachzeitschriften und auf Internet-Seiten sowie auf entsprechende Zertifizierungsreports.

Für die Sicherheitszertifizierung von IT-Produkten ist das BSI (www.bsi.de/zertifiz/zert/) eine gute Anlaufstelle. Dort finden Sie Zertifizierungsreports zum Download sowie in den Broschüren 7148 und 7149 Links zu anderen Zertifizierungsstellen im In- und Ausland mit weiteren Informationen. Sie werden überrascht sein, wie viele IT-Produkte aus allen Bereichen evaluiert und zertifiziert worden sind.

Wie man an aktuelle Informationen zu Schwachstellen von Produkten, Systemen und Sicherheitsmaßnahmen kommt, haben wir in Abschnitt 5.5 behandelt.

Informationen über Infrastruktursicherheit und geeignete Produkte finden Sie insbesondere auf den Web-Seiten (www.vds.de, Menüpunkt „VDS-Anerkennungen“) des Verbands der Sachversicherer (VdS).

Normung

Das Thema Informationssicherheit hat einen erheblichen Einfluss auf die nationale und internationale Normung. Wenn Sie spezielle Normen suchen, können Sie erste Informationen bei den Normungsgebern wie DIN, ETSI, IEEE und ISO finden. Anlaufstelle für (fast immer nur gegen Gebühr) zu beschaffende Normen in Deutschland ist der Beuth-Verlag (www.beuth.de).

Internet-Sicherheit

Aus Gründen des Umfangs haben wir das Thema Internet-Sicherheit nicht in aller Ausführlichkeit ansprechen können. Hierzu existiert eine große Zahl von Fachbüchern – es sei aber zum Einstieg auf eine ältere Studie des BSI verwiesen, die kostenlos zum Download[57] bereit steht und einen guten Überblick über das Thema bietet.

Elektronische Signatur

Für alles, was im Zusammenhang mit der elektronischen Signatur steht, ist die Bundesnetzagentur (www.bundesnetzagentur.de) erste Anlaufstelle, sodann die von ihr zugelassenen Prüf- und Bestätigungsstellen, die auf den genannten Web-Seiten der BNetzA (Stichwort „Elektronische Signatur“) aufgeführt sind.

Der TeleTrusT Deutschland e.V. (www.teletrust.de) bietet interessante Informationen zur Vertrauenswürdigkeit von Informations- und Kommunikationstechnik, z. B. über Kryptografie, Biometrie und die elektronische Signatur.

Zertifizierung

Viele Unternehmen gehen den Weg, ihre Sicherheit regelmäßig auditieren zu lassen – und zwar zumindest durch eigene (interne) Audits. Als Nachweis für Aufsichtbehörden, Banken (im Zusammenhang mit Basel II) und letztlich auch für Kunden hat sich die *externe* Auditierung und Zertifizierung als sinnvoll herausgestellt; sie wird in zunehmenden Maße nachgefragt.

Als mögliche Vorgabe kommt dafür die ISO 27001 – in Deutschland ggf. in Verbindung mit dem IT-Grundschutz – in Frage.

Falls Sie solche Auditierungen anstreben, wird empfohlen, mit einschlägigen Auditoren und Zertifizierungsstellen in Kontakt zu treten. Hierbei hilfreich sind die entsprechenden Listen der Akkreditierungsgeber wie z. B. der DATech (www.datech.de), der TGA (www.tga-gmbh.de) und dem BSI (www.bsi.de/gshb/zert/), die Namen von lizenzierten Auditoren und akkreditierten Zertifizierungsstellen enthalten.

Zusätzlich zu den genannten Normen haben einige Zertifizierungsstellen[58] eigene Vorgaben und Verfahren entwickelt, die kundenspezifisch angepasst oder zur Zertifizierung der Sicherheit von Geschäftsprozessen angewendet werden können.

Nochmal PDCA

Werfen wir noch einen Blick auf das eingangs behandelte PDCA-Modell und die Aktivitäten *Plan1* und *Plan2*, die die Sensibilisierung und Schulung des Sicherheitsmanagements zum Gegen-

57 unter www.bsi.de/literat/studien/firewall/fwstud.htm

58 s. beispielsweise www.tuvit.de, www.t-systems-zert.com

stand haben. Das gängige „Medium“ wird hier der Besuch von Sicherheitstagungen und Seminaren sein, die nicht nur unter dem Gesichtspunkt „Weiterbildung“, sondern vor allem wegen des möglichen Erfahrungsaustauschs unter Sicherheitsverantwortlichen dringend empfohlen werden. Eine regelmäßige Teilnahme an solchen Veranstaltungen ist deshalb für Sicherheitsverantwortliche ein „muss“.

Sicherheitsberater

Es soll nicht unerwähnt bleiben, dass sich gerade im Gebiet der Informationssicherheit eine große Zahl von Sicherheitsberatern betätigt, die Unternehmen beim Aufbau und Betrieb ihres Sicherheitsmanagements unterstützen können. Wesentlich ist hier der Aspekt, im Bedarfsfall Berater auszuwählen, die eine Neutralität gegenüber Herstellern und deren Produkten wahren und somit eine *unabhängige* Beratung leisten können. Man erkennt dies z. B. daran, dass für bestimmte Fragestellungen Lösungen verschiedener Hersteller vorgeschlagen werden, oder daran, dass es sich um Institutionen handelt, die durch eine Akkreditierung eine formelle (durch Dritte überwachte) Neutralität nachweisen können.

Als letztes…

Sicherheit in dem hier gemeinten Sinne ist nichts, was gleich beim ersten Mal in einem „großen Wurf“ gelingt, sondern einige Zeit – eher Jahre als Monate – benötigt, bevor man eine Art „stabile Lage“ erreicht. Wichtig ist dabei, sich immer an der Idee der kontinuierlichen Verbesserung (das Anliegen des PDCA-Modells) zu orientieren und schrittweise vorzugehen.

Abbildungsverzeichnis

Tabellenverzeichnis

Verwendete Abkürzungen

ACL	Access Control List
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur (früher: RegTP)
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBT	Computer Based Training
CC	Common Criteria
CERT	Computer Emergency Response Team
CPU	Central Processing Unit
CSP	Certification Service Provider
DAC	Discretionary Access Control
DATech	Deutsche Akkreditierungsstelle Technik e.V., neuer Name: DATech in der TGA GmbH
DES	Data Encryption Standard
DIN	Deutsche Institut für Normung e.V.
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EN	European Norm
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
HF	Hochfrequenz
IC	Integrated Circuit
ICV	Integrity Check Value

ID	Identifikation
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IEEE	Institute of Electrical and Electronics Engineers Inc.
ISF	Information Security Forum
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
IV	Informationsverarbeitung, informationsverarbeitendes…
KMU	Kleines, mittelständisches Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LAN	Local Area Network
MAC	Mandatory Access Control
MDStV	Mediendienste-Staatsvertrag
MTBF	Mean Time between Failure
NDA	Non Disclosure Agreement
PDCA	Plan-Do-Check-Act
PDF	Portable Document Format
PIN	Personal Identification Number

PUK	Personal Unblocking Key
QM	Quality Management
RAID	Redundant Array of Inexpensive (Independent) Disks
RCx	Rivest Cipher
RFC	Request for Comments
RFID	Radio Frequency Identity Tags
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROSI	Return on Security Investment
RSA	Rivest-Shamir-Adleman
RZ	Rechenzentrum
SAK	Signaturanwendungskomponente
SD	Single Density
SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SOX	Sarbanes Oxley Act
SSID	Service Set Identifier (Network Name)
SSL	Secure Socket Layer
SW	Software
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Evaluation Criteria
TDDSG	Teledienstedatenschutzgesetz
TGA	Trägergemeinschaft für Akkreditierung GmbH
TK	Telekommunikation(s-)
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USV	unterbrechungsfreie Stromversorgung
VdS	Verband der Sachversicherer
VoIP	Voice over IP

WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WK	Widerstandsklasse
WLAN	Wireless LAN (Local Area Network)
WPA	Wi-Fi Protected Access
WWW	World Wide Web
ZDA	Zertifizierungsdiensteanbieter

Fachbegriffe deutsch ./. englisch

Assets (Value~, Information~)	(Informations-)Werte auch: Schutzobjekte
Availability	Verfügbarkeit
Awareness (Security~)	(Sicherheits~) Bewußtsein
Change Management	Änderungsmanagement
Compliance	Einhaltung von Vorgaben
Confidentiality	Vertraulichkeit
Control Objectives	Maßnahmenziele
Controls	Anforderungen (an Maßnahmen)
Discretionary Access Control	benutzerbestimmbare Zugriffskontrolle
Exploitation	Ausnutzbarkeit (z. B. von Schwachstellen)
Frequency	Häufigkeit
Incident (Security~)	(Sicherheits-)Vorfall
Integrity	Integrität
IT Security Manager	IT-Sicherheitsbeauftragte(r)
Likelihood	(Eintritts-)Wahrscheinlichkeit
Management Review	Management-Bewertung
Mandatory Access Control	vorgeschriebene Zugriffskontrolle
Non Repudiation	Nicht-Abstreitbarkeit
Privacy	Privatsphäre (dazu gehörend: die personenbezogenen Informationen)
Protection Effect	Schutzwirkung
Quality Management	Qualitätsmanagement

Replay Attack	Angriff durch Wiedereinspielen von abgehörten Daten
Reporting	Berichtswesen
Requirements (Security~)	Anforderungen (Sicherheits~)
Residual Risk	Restrisiko
Risk Analysis	Risikoanalyse
Risk Assessment	Risikoeinschätzung
Risk Estimation	Risikoabschätzung
Risk Evaluation	Risikobewertung
Risk Identification	Risiko-Identifizierung
Safeguards	Sicherungs-, Schutzmaßnahmen
Scope	Anwendungsbereich
Security Policy	Sicherheitsleitlinie[59]
Self-Assessment	Selbsteinschätzung
Statement of Applicability	Erklärung zur Anwendbarkeit bzw. zur Eignung
Threat	Bedrohung
Vulnerability	Verletzlichkeit, (ausnutzbare) Schwachstelle
Weakness	Schwachstelle

[59] fälschlicherweise oft als „Sicherheitspolitik“ übersetzt

Quellenhinweise

/BS 7799-2/	BS 7799-2:2002 Specification for Information Security Management, www.bsi-global.com
/BSI100-1/	Managementsysteme für Informationssicherheit (ISMS), BSI, www.bsi.de/gshb
/BSI100-2/	IT-Grundschutz-Vorgehensweise, BSI, www.bsi.de/gshb
/BSI100-3/	Risikoanalyse auf der Basis von IT-Grundschutz, BSI, www.bsi.de/gshb
/BSI-G/	IT-Grundschutz: Gefährdungskataloge, BSI, www.bsi.de/gshb
/BSI-M/	IT-Grundschutz: Maßnahmenkataloge, BSI, www.bsi.de/gshb
/CC/	Common Criteria for Information Technology Security Evaluation, www.commoncriteriaportal.com
/CEM/	Common Methodology for Information Technology Security Evaluation, www.commoncriteriaportal.com
/DIN EN 50173/	Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen, www.din.de
/DIN V EN 1627/	Fenster, Türen, Abschlüsse – Einbruchhemmung – Anforderungen und Klassifizierung, www.din.de
/IEEE 802.11/	IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, www.ieee.org
/IS0 7816/	ISO/IEC 7816-x Identification Cards, www.iso.org

/ISO 15408/	ISO/IEC 15408: Fassung der /CC/ als internationale Norm
/ISO 17799/	ISO/IEC 17799: Information technology – Security techniques – Code of practice for information security management, www.iso.org
/ISO 27001/	ISO/IEC FDIS 27001: Information technology – Security techniques – Information security management systems – Requirements, www.iso.org
/ISO 73/	ISO / IEC Guide 73:2002 Risk management – Vocabulary – Guidelines for use in standards
/ITIL/	Information Technology Infrastructure Library, z. B. Informationen unter http://www.itsmf.de/
/ITSEC/	Information Technology Security Evaluation Criteria, www.bsi.de
/ITSEM/	Information Technology Security Evaluation Manual, www.bsi.de
/KRS2008/	Kersten H., Reuter J., Schröder K.W.: „IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung“, Vieweg Verlag, 2008, ISBN 978-3-8348-0178-4
/SigG/	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, www.bundesnetzagentur.de, Link: „Elektronische Signatur/Rechtsvorschriften“
/SigV/	Verordnung zur elektronischen Signatur, www.bundesnetzagentur.de, Link: „Elektronische Signatur/Rechtsvorschriften“
/TCSEC/	Trusted Computer System Evaluation Criteria, http://csrc.nist.gov/publications

Sachwortverzeichnis

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z