Jochen Brunnstein

ITIL Security Management realisieren

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 SecuMedia 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.

Die ersten Titel der Reihe:

Praxis des IT-Rechts
Von Horst Speichert

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

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

Der IT Security Manager
Von Heinrich Kersten und Gerhard Klett

ITL Security Management realisieren
Von Jochen Brunnstein

www.vieweg.de

Jochen Brunnstein

ITIL Security Management realisieren

IT-Service Security Management nach ITIL – So gehen Sie vor

Mit 40 Abbildungen

vieweg

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

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

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

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

1. Auflage September 2006

Alle Rechte vorbehalten
© Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden 2006

Lektorat: Günter Schulz / Andrea Broßler

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

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

Konzeption und Layout des Umschlags: Ulrike Weigel, www.CorporateDesignGroup.de
Umschlagbild: Nina Faber de.sign, Wiesbaden
Druck- und buchbinderische Verarbeitung: MercedesDruck, Berlin
Printed in Germany

ISBN-10 3-8348-0165-8
ISBN-13 3-8348-0165-4

Vorwort

Wie kaum eine andere Technik zuvor haben sich Informations- und Kommunikationstechniken verschiedenster Art nahezu explosionsartig in Unternehmen und Organisationen ausgebreitet. Diese Entwicklung, angeblich vom Markt getrieben, ist zwar von den Vorständen vieler Unternehmen wegen ihrer innovativen und rationalisierenden Wirkungen oft gewollt, aber mangels Verstehens der diesen zugrunde liegenden Prozessen meist unzureichend gesteuert worden. Ebenfalls mangels systematischer Planung und Überwachung bei der Einführung von IT-Verfahren hat sich vielerorts ein Wildwuchs an DV- und IT-Systemen entwickelt, welche neben unzureichender Kompatibilität vor allem erhebliche Schwachpunkte – etwa geringem Widerstand gegen Angriffe von außen und innen sowie vor allem häufige Ausfälle oder Fehlfunktionen wichtiger Teilsysteme – zu schwer versicherbaren Risiken werden lassen. Dabei erweisen sich besonders die Internet-gestützten Verbindungen innerhalb der Unternehmen sowie zu Lieferanten, Kunden und dritten Partnern (etwa der Steuerverwaltung) als besondere Angriffspunkte, welche zunehmend – ob mit lustvollem Hacking oder krimineller Energie – die Existenz und Profitabilität von Unternehmen gefährden.

Gegen diese Entwicklung versuchen interessierte Kreise seit langem, vermeintlich „sichere Software und Systeme“ zu entwickeln und am Markt durchzusetzen. Lange Zeit hielt man es für zweckmäßig und ausreichend, für derartige Systeme einen „Sicherheitsgrad“ zu definieren, wobei man Kriterienkataloge zugrunde legte. Während sich die Kataloge der „Spectral Series“, darunter das bekannte „Orange Book“ (Trusted Computer Security Evaluation Criteria, mit Sicherheitsgraden von C1 bis A) für die Sicherheit einzeln stehender Systeme, vor allem – gemäß den Interessen des militärisch-staatlichen Nationalen Computersicherheitszentrums der USA – an der Durchsetzung der Vertraulichkeit orientierten, haben spätere Ansätze – das deutsche Green Book, die Europäischen „IT-Sicherheitskriterien“ sowie aktuell die sog. „Common Criteria“ – versucht, die Einstufung der Sicherheit von IT-Produkten auf weitere, vor allem für Unternehmen interessante Anforderungen wie „Integrität“ und „Verfügbarkeit“ auszuweiten sowie Anforderungen der Anwender – Stichwort: Sicherheitsprofil – ins Spiel zu bringen. Leider haben diese Kriterien kaum zum Entwurf sicherer IT-Systeme und Produkte beigetra-

gen, zumal nicht einmal deren Lebenszyklen, geschweige denn Anforderungen an den Einsatz in Unternehmen berücksichtigt wurden.

Bei der Konzentration auf vermeintlich sichere Systeme wurde nämlich übersehen, dass Planung und Einsatz von IT-Systemen in Unternehmen sich in zeitlichen Folgen (Lebenszyklen) entwickeln, welche ein methodisches Vorgehen erfordern. Seit einiger Zeit werden daher die Prozesse, welche den Einsatz von I&K-Systemen in Unternehmen steuern, auf der Anwender- und Beraterseite (wenn auch kaum bei den Systemherstellern) besonders betrachtet. Von der Erfassung wesentlicher Daten (wie im Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik, BSI) bis zu den Darstellungen der „Besten Praktischen Verfahren“ (Best Practices, BS 7799 des British Standard Institutes, BSI und daraus abgeleitet die ISO 17799) reicht ein breites Spektrum von Vorschlägen, wie die Planung und der Einsatz moderner I&K-Systeme sachgerecht und mit möglichst hohen Gewinnen an Funktionalität, Verlässlichkeit und IT-Sicherheit gesteuert werden kann.

Im Rahmen dieser Betrachtungen stellt ITIL, die „Information Technology Infrastructure Library“ einen Quasi-Standard dar, welcher Unterstützung und Handreichungen vor allem für die Praktiker im Unternehmen beiträgt. Dabei wird auch die Leitungsebene einbezogen, welcher durch neuere Regelungen (vom Risikomanagement á la KonTraG bis Sarbanes Oxley) auch eine zunehmende Verantwortung hinsichtlich der Gewährleistung der IT-Sicherheit abverlangt wird. Das hier vorgelegte Buch hat sich zur Aufgabe gemacht, die Anforderungen auf den Ebenen der Dienste (service level) und ihrer Verfügbarkeit (availability) und ausreichender Kapazität wie auch bei der Zusicherung der Kontinuität der Geschäftsprozesse darzustellen und mit sinnfälligen Fallbeispielen der „Best Practice“-Kategorie zu illustrieren. Dabei werden die verschiedenen Phasen, die in anderen Betrachtungen vernachlässigt werden, herausgearbeitet (control, plan, do, check, act).

Ein wichtiger Beitrag dieses Buches besteht sicherlich darin, dass es die vielerorts dominierende Sicht der IT-Sicherheitsexperten zurückdrängt, um stattdessen die Bedürfnisse von Unternehmen in den Vordergrund zu stellen. Dieser praktische Leitfaden kann und möge daher helfen, die oft unzureichende Produkt- und Systemsicherheit durch angepasstes, an Musterbeispielen orientiertes Handeln zu kompensieren. Insofern möge diesem Buch eine gute Rezeption beschieden sein.

Hamburg, im Juli 2006

Dr. Klaus Brunnstein

Professor (a.D.) für Anwendungen der Informatik

Universität Hamburg

Vorwort des Verfassers

Information ist nach Arbeit, Boden und Kapital der vierte Produktionsfaktor.

Während Arbeit, Boden und Kapital in der Gesellschaft als schützenswert empfunden werden, wird die Auswirkung von Angriffen auf Informationen stark unterschätzt.

Dabei sind es in immer stärkerem Maße die Informationen, die Unternehmen einen Wettbewerbsvorteil verschaffen, oder dazu führen, dass sich neue Geschäftsfelder ergeben.

Jedes Unternehmen hat Informationen, die es schützen muss, sei es aus gesetzlichen Gründen, beispielsweise dem Datenschutz, oder aus eigenem Antrieb.

Der Datenschutz wird dabei leider oft nur halbherzig berücksichtigt. Aber auch der Schutz der eigenen Daten wird in Unternehmen häufig Systemlösungsanbietern überlassen. Diese sind Anbieter von speziellen Lösungen zum Übertragen oder Speichern von Daten, aber auch spezialisierte Hersteller von Software, die einzelne Sicherheitsprobleme bekämpft, wie beispielsweise Firewalls oder Anti-MalWare.

Immer mehr Anbieter haben integrierte Sicherheitssuiten in ihrem Verkaufskatalog, die den Kunden Rundum-Glücklich-Pakete versprechen.

Solche Standardlösungen werden stark mit der schnellen Einsatzmöglichkeit (Effizienz) beworben, sollten jedoch mit Vorsicht und Verstand ausgewählt werden, denn nicht immer passt das Angebot mit den tatsächlichen Gegebenheiten des geschäftlichen Alltags zusammen.

Werkzeuge, und das sind solche Softwarelösungen, müssen immer mit Sachverstand genutzt werden. Das setzt voraus, dass die Werkzeuge nur im Rahmen eines Verfahrens nach klar definierten Vorschriften eingesetzt werden und, dieses gilt speziell für die Informationsverarbeitung, dass der Einsatz sich an Ablaufplänen darüber orientiert, wann welches Werkzeug wie benutzt werden kann.

Solche Ablaufpläne sind Prozesse.

Dieses Buch beschreibt den Prozess des IT Security Managements, gemäß dem De-facto-Standard ITIL (Information Technology Infrastructure Library).

Es wurde bewusst ein praktischer Ansatz mit vielen Beispielen gewählt, so dass die Anpassung an eigene Anforderungen erleichtert wird.

In diesem Buch wird von Unternehmen gesprochen. Alle gemachten Ausführungen treffen jedoch auch auf andere Organisationsformen sowie die öffentliche Verwaltung zu.

In diesem Buch werden viele englische Begriffe verwendet. Dies ist bei einem Fachbuch über Informationstechnologie leider nicht vollständig auszuschließen. Ich habe mich jedoch bemüht, diese Begriffe auf Deutsch zu erläutern. Weiterhin gibt es ein ausführliches Glossar, das die Begriffe erklärt.

Ich möchte an dieser Stelle besonders den Menschen danken, die mit Ideen, Anregungen, Kritik und Ermunterung zum Gelingen dieses Buches beigetragen haben,

meiner Frau Nicole für viele Stunden Korrekturlesen, die Geduld und den Ansporn,

meinen Kindern, Rebekka, Isabel und Tim für ihre Geduld und Unterstützung,

meinem Vater, Klaus Brunnstein für die fachliche Unterstützung, seinen Rat und das Vorwort,

meiner Mutter, Gunda Brunnstein, die mich immer unterstützt hat,

Wolf-Dieter Jahn, meinen Mentor in die Welt der IT-Sicherheit,

sowie meinen Kollegen und Kunden, die meine Sicht auf die Informationssicherheit immer wieder erweitert haben.

Wedel, im Juli 2006 Jochen Brunnstein

Inhaltsverzeichnis

1 Einleitung

Der Begriff IT-Sicherheit ist irreführend, da es nicht um die Sicherheit, also den Schutz von Informationstechnologie geht. Vielmehr handelt es sich um den Schutz von Informationen, die elektronisch als Daten gespeichert und mithilfe von Informationstechnologie verarbeitet werden.

Diese Informationen werden bedroht, manchmal durch die Anwender, verstärkt aber durch MalWare, Hacker, Wirtschaftsspione und Kriminelle.

Während die Gefahren für die Informationen zunehmen, wächst die Abhängigkeit von der IT. Durch die hochgradige Abhängigkeit wächst die Angst vor Informationsmissbrauch und der Ruf nach Schutzmaßnahmen wird lauter.

Das Wort Maßnahmen ist für viele gleichbedeutend mit Tools, weshalb die Anzahl der eingesetzten Sicherheitslösungen stark ansteigt. Je mehr Tools eingesetzt werden, desto geringer ist die Beherrschbarkeit und die Transparenz sinkt, so dass die Gefahr wieder steigt, eine Bedrohung zu übersehen.

Hohe Abhängigkeit von der IT ohne Beherrschbarkeit derselben bedeutet Unsicherheit.

Parallel zu dieser Entwicklung geraten die IT-Budgets stark unter Druck, obwohl die Aufgaben fast täglich zunehmen. In Zeiten knapper Kassen müssen Prioritäten gefunden werden und Maßnahmen werden nur dann implementiert, wenn diese die Geschäftsprozesse verbessern oder zu einem Wettbewerbsvorteil führen.

Der interne Wettbewerb mit anderen Projekten um knappe Budgets fordert von der Informationstechnologie ebenfalls ein hohes Maß an Transparenz über Nutzen und Kosten.

Einerseits werden häufig nur noch strategische Projekte mit entsprechenden Budgets ausgestattet, andererseits soll der Aufwand für Aufgaben des Tagesgeschäftes immer stärker zurückgefahren werden.

Unternehmen suchen hier praxisbewährte, so genannte Best Practice Lösungen, die bereits vielfach erfolgreich eingesetzt

worden sind und einen großen Teil der Anforderungen abdecken.

Dies gilt für IT-Services, aber immer stärker auch für Verfahren, Prozesse und Organisationsformen.

Häufig werden Projekte nur noch dann gestartet, wenn ein Benchmark mit dem Wettbewerb ergibt, dass dieser besser aufgestellt ist.

Um jedoch einen aussagekräftigen Benchmark durchführen zu können, müssen vergleichbare Bewertungskriterien ausgewählt werden. Auch hierbei helfen Best Practice Standards.

1.1 Status Quo der Informationssicherheit

Informationssicherheit (IS) ist heute nach wie vor zumeist eine reaktive Beschäftigung mit bereits aufgetretenen Sicherheitsvorfällen (Security Incidents). Unabhängig davon, ob die Sicherheitsvorfälle im eigenen Unternehmen oder bei anderen aufgetreten sind, ist der gängige Ansatz, erst dann auf eine Gefahr zu reagieren, wenn daraus eine Bedrohung geworden ist. Dieses gilt nicht nur für die Anwenderunternehmen, sondern im großen Maße auch für die Herstellerunternehmen. Viele Bedrohungen für die Informationssicherheit könnten vermieden werden, wenn Hersteller von Software und Hardware frühzeitig auf Warnhinweise reagierten. Die Liste solcher Herstellerunternehmen ist lang und lässt keine Branche und kein Land aus.

Hier liegt eines der Hauptprobleme, nämlich dass die Informationssicherheit als eigenständige Disziplin angesehen wird.

Informationssicherheit ist aber nur ein Qualitätsaspekt, der durch Hersteller und Anwenderunternehmen sichergestellt werden muss.

Qualität bedeutet die Erfüllung der Anforderungen oder Erwartungshaltung, die an bestimmte Merkmale besteht.

Dies bedeutet, dass die Anforderung an die Informationssicherheit bekannt sein muss, und zwar in Bezug auf alle drei Merkmale der Informationssicherheit:

- Vertraulichkeit
- Verfügbarkeit
- Integrität.

Qualitätsmanagement bedeutet die Sicherstellung der Qualitätsziele durch geeignete Maßnahmen. Durch Prüfungen, ob die Anforderungen an die Informationssicherheit eingehalten werden (Qualitätssicherung) wird die Ausprägung der Merkmale gemessen. Als Ergebnis der Qualitätssicherung werden die Maßnahmen zur Erreichung der Merkmale optimiert und somit wird ein Qualitätskreislauf am Laufen gehalten.

Dieser sehr kurz gehaltene Kreislauf findet sich später im Kapitel über Security Management wieder, dann allerdings auf die Qualitätsmerkmale der Informationssicherheit abgestimmt.

Diese erweiterte Sicht des Qualitätsmanagements fehlt vielen Unternehmen, so dass die Möglichkeit einer frühzeitigen Einbindung von Security Experten beispielsweise in Entwicklungsprojekte heute bedauerlicherweise noch immer längst nicht im ausreichenden Maße genutzt wird.

1.2 Zielgruppe

Dieses Buch soll all denen als Übersicht und Leitfaden dienen,

- die Informationssicherheit verantworten und sich die Frage nach Optimierungspotentialen und Best Practice Ansätzen stellen,
- die Informationssicherheit operativ umsetzen und eine ganzheitliche Übersicht über die Komplexität von Informationssicherheit erlangen möchten,
- die Informationssicherheit prüfen und in kurzer Zeit zu verlässlichen und belastbaren Aussagen kommen müssen,
- die Informationssicherheit als Bestandteil ihrer Aufgabe erkannt haben und sich einen Überblick über die Aufgaben der Informationssicherheit verschaffen möchten.

1.3 Was ist das Buch nicht?

Dieses Buch ist keine Einführung in das Thema ITIL. Um einen guten Überblick über ITIL zu erlangen kann die Lektüre der Bücher „ITIL kompakt und verständlich“, sowie „Optimiertes IT-Management mit ITIL“ empfohlen werden. Beide Bücher sind im Vieweg Verlag erschienen und vermitteln sehr gut, was ITIL ist und wie es von Unternehmen genutzt werden kann.

Dieses Buch ist auch kein Kochbuch, das Wort für Wort umgesetzt werden muss. Jedes Unternehmen hat eine eigene gewachsene Kultur, daher sind Organisationsformen, Kommunikationsverhalten und Verantwortlichkeit sehr unterschiedlich. Ein Security Management kann jedoch nur dann erfolgreich sein, wenn all diese Aspekte berücksichtigt werden und das Security Management nicht wie ein Fremdkörper von außen übergestülpt wird. Durch den starken Praxisbezug wird dem Leser aber ein guter Weg beschrieben, um ein Security Management erfolgreich einzuführen.

Weiterhin eignet sich das Buch nicht als Blaupause für die Auswahl von Sicherheitswerkzeugen, wie zum Beispiel Firewalls, Anti-MalWare Programmen oder Intrusion-Prevention-Systemen.

1.4 Make or Buy

Die Standardfrage im Umfeld Security Management lautet:

Kaufe ich mir einen Standard oder entwickle ich meinen Prozess eigenständig?

Im Softwarebereich nennt man den Kauf von standardisierten Komponenten Commercial-off-the-Shelf[1] Software (CotS). Hintergrund eines solchen Kaufes ist die Überlegung, dass die eigenen Geschäftsprozesse eine hohe Allgemeingültigkeit besitzen und Software, die bei anderen Unternehmen gute Dienste leistet, dieses auch im eigenen Hause tun wird.

Wenn man dieses Prinzip auf das Security Management anwendet, würden hier Berater mit der Implementierung beauftragt werden, die einen gültigen Standard in ihrem eigenen Werkzeugkoffer mitbringen und durch Anpassung fertiger Vorlagen an das Unternehmen einen Prozess in kürzester Zeit, mit geringstem Aufwand und hoher Passgenauigkeit implementieren.

Dass die Welt der Prozesse und Beratungshäuser anders aussieht zeigen uns viele Projekte aus den unterschiedlichsten Bereichen. Nur mit dem nötigen Maß an Kenntnis der Kultur innerhalb des Unternehmens, sowie der tatsächlich gelebten Geschäftsprozesse können Prozesse implementiert werden. Dieses gilt in besonderem Maße für das Security Management.

Folgende Gründe gibt es für einen CotS-Ansatz:

- Wirtschaftlichkeit
- Kurze Implementierungszeit
- Hohes im Markt vorhandenes Knowhow
- Vergleichbarkeit mit anderen Unternehmen

Das Gegenteil vom CotS ist die 100%ige Individuallösung. Diese Lösung wird häufig von Unternehmen gewählt, die ihre Geschäftsprozesse als so individuell ansehen, dass eine Nutzung von Standards nicht in Frage kommt.

Die Vorteile dieser Lösung sind:

- Starke Unterstützung seitens des Managements

[1] Aus dem Verkaufsregal

- Stellenwert von Sicherheit wurde vom Unternehmen erkannt
- Akzeptanz von Neuerungen
- Hohes Maß an Sicherheit

Beide Ansätze haben Vor- und Nachteile, jedoch hat sich in vielen Projekten als gute Lösung ein Mittelweg ergeben, der folgende Erfolgsfaktoren berücksichtigt:

- Aus wirtschaftlichen Gründen sollten so viele Standards wie möglich genutzt werden. Bei allem, was nicht individuell entwickelt worden ist, muss immer auf die Erweiterbarkeit und Wartbarkeit geachtet werden, damit zukünftige Entwicklungen später noch mit demselben Verfahren arbeiten können,
- An kritischen Stellen müssen eigene Ergebnisse, Anforderungen und Verfahren berücksichtigt werden,
- Es sollten so viele bereits genutzte Verfahren wie möglich in den Prozess eingehen, da dann ein hohes Maß an Wieder-erkennung durch die Anwender gegeben ist,
- Der Prozess sollte nicht erst starten, wenn 100% aller Verfahren beschrieben und alle Abschlussveranstaltungen gehalten worden sind. Eine schrittweise Einführung lässt dem Security Management Prozess und den Anwendern eine Gewöhnungszeit. Häufig kann mit den ersten 20% Aufwand bereits viel von den ersten 80% Ergebnis erzielt werden.

Häufig werden ITIL Projekte mit der Einführung von Tools verbunden. Hier gilt das oben beschriebene analog, gemäß der alten Weisheit: „A fool with a tool is still a fool“.

Die Einführung eines Werkzeuges ohne einen Prozess, speziell im Umfeld der Informationssicherheit, kann niemals eine dauerhafte Lösung sein, sondern nur kurzfristig Defizite bekämpfen.

2 Security Management

Im nachfolgenden Kapitel wird der Security Management Prozess vorgestellt. Weiterhin werden die grundsätzlichen Begriffe der Informationssicherheit erläutert und die Frage beantwortet, warum Unternehmen einen Security Management Prozess etablieren und leben sollten.

2.1 Grundlagen der Informationssicherheit

Informationssicherheit (IS) ist kein Selbstzweck, sonder eine Sammlung von Qualitätsmerkmalen, die ein Unternehmen definieren muss.

Unternehmen benötigen für ihre Geschäftstätigkeit Informationen, sei es für die Produktion von Gütern, die Erbringung von Dienstleistungen oder Aufgaben der öffentlichen Hand. Diese Informationen wurden seit jeher benötigt, beispielsweise Informationen über Kunden, Lieferanten und interne Abläufe. Durch den Einsatz von Informationstechnologie (IT) wurden die Verarbeitungsgeschwindigkeit und die Menge der Informationen vervielfacht. Unverändert ist jedoch die Tatsache, dass Informationen nur dann wichtig und damit schützenswert sind, wenn die Geschäftsprozesse diese Informationen benötigen.

Die einzelnen Geschäftsprozesse wiederum werden aus den übergeordneten Unternehmenszielen abgeleitet. Die Geschäftsprozesse stellen Anforderungen an die Informationen in Form von Qualitätsmerkmalen. Einer der Gründe, warum nur etwa 29% aller IT Projekte erfolgreich sind[2] ist die Tatsache, dass die Art und Weise der Formulierung von Anforderungen unzureichend ist. Fachbereiche sprechen „Business-Deutsch“, IT-Bereiche sprechen „IT-Deutsch“. Häufig herrschen daher babylonische Zustände, und kaum einer versteht den anderen. Die Idee, die Fachbereiche qua Modellierungsverfahren á la UML[3] in die IT-Diktion einzubeziehen ist bislang noch ein nicht abgeschlossener Versuch

[2] Quelle: Chaos Report 2004, The Standish Group

[3] Unified Modelling Language

mit offenem Ende, löst jedoch im besten Fall nur die Krux der funktionalen Anforderungen.

Ein ebenso wichtiger Block ist die Anforderung an nichtfunktionale Qualitätsmerkmale, wie zum Beispiel IS, Wartbarkeit, Benutzbarkeit, Performance und Belastbarkeit.

An dieser Stelle setzt das Security Management an, indem es die Qualitätsmerkmale der IS plant, unterstützt und überwacht. Diese Qualitätsmerkmale sind folgende:

Vertraulichkeit (engl. Confidentiality) bedeutet, dass nur berechtigte Personen und Systeme auf Informationen Zugriff erhalten.

Integrität (engl. Integrity) stellt das Maß dar, in dem Informationen richtig gespeichert sind, verarbeitet oder übertragen werden. Richtig bedeutet hier, dass die Informationen nicht unbefugt und unbeabsichtigt verändert werden, wie dieses beispielsweise MalWare tut.

Verfügbarkeit (engl. Availability) beschreibt den Grad, inwiefern IT-Service in einem definierten Zeitraum zur Nutzung zur Verfügung stehen.

Neben diesen Hauptmerkmalen gibt es noch einige weitere IS-Qualitätsmerkmale, die manchmal benötigt werden. Die häufigsten dieser untergeordneten Qualitätsmerkmale sind folgende:

- Authentizität (engl. Authenticity)
- Unleugbarkeit (engl. Non-Repudiation)
- Vertrauenswürdigkeit (engl. Trustworthiness)
- Zurechenbarkeit (engl. Accountability)

Während eine Information nur dann als sicher im Sinne der IS gilt, wenn Vertraulichkeit, Integrität und Verfügbarkeit definiert sind und im geforderten Maße gewährleistet werden können, sind die untergeordneten Qualitätsmerkmale nur dann verbindlich, wenn diese von bestimmten Geschäftsprozessen definiert worden sind.

- Für einen Webshop ist es wichtig, die Authentizität eines Käufers feststellen zu können, um das Risiko zu minimieren, dass ein Dritter im Namen und auf Rechnung eines Kunden eine Bestellung tätigt.
- Bei der Übermittlung einer elektronischen Willenserklärung, zum Beispiel bei rechtsverbindlichen Geschäften über das Internet, muss sichergestellt werden, dass der Versender diese elektronische Erklärung auch tatsächlich abgegeben hat (Non-Repudiation of Origin) und dieses später nicht leugnen kann. Ebenso muss auch sichergestellt werden, dass der Empfänger diese Willenserklärung auch tatsächlich erhalten hat (Non-Repudiation of Delivery).

Nachdem alle Qualitätsmerkmale definiert worden sind, müssen die eingesetzten Betriebsmittel (Hardware, Software) und die Informationen hinsichtlich dieser Qualitätsmerkmale gemäß der Anforderung klassifiziert werden. Die Klassifizierung sorgt dafür, dass der Aufwand zum Schutz von Informationen immer einen Bezug zum Nutzen hat. Auf Basis dieser Klassifikation werden Maßnahmen geplant und implementiert.

Das Security Management überwacht diese Maßnahmen und meldet durch ein aussagekräftiges Berichtswesen der Unternehmensleitung zurück, wie gut die Sicherheitsziele erreicht worden sind und damit die übergeordneten Unternehmensziele unterstützt haben.

Ziel dieses Prozesses ist eine auf ein Unternehmen maßgeschneiderte IS.

2.2 Woher kommen die Vorgaben?

Der erste Schritt ist häufig sehr schwierig. Beim Security Management ist dies die Identifikation der Anforderungen.

1. Wer stellt die Anforderungen?
2. Welche Anforderungen werden gestellt?
3. Sind diese Anforderungen für die IS relevant?

Die Liste derjenigen, die Anforderungen stellen können ist allgemein gültig und gilt damit auch für die Anforderungen an die IS.

- Staat
- Gesellschaft
- Markt
- Unternehmen

Die Reihenfolge soll bei dieser Auflistung keinen Stellenwert ausdrücken, wobei der Staat sicherlich einen sehr großen Einfluss darauf hat, ob Vorhaben und Projekte von Unternehmen durchgeführt werden oder nicht. Einen ähnlich großen Einfluss haben die Organisationen, die Kreditvergaberichtlinien festlegen, wie beispielsweise die BASEL II Richtlinie.

Die Anforderungen des Staates bestehen aus Gesetzen und Verordnungen. Einige Anforderungen des Staates werden proaktiv eingefordert, beispielsweise die Einhaltung der Abgabenordnung (AO). Andere werden stichprobenartig und unregelmäßig auf Einhaltung geprüft. Dritte werden nur auf Antrag oder bei schlimmen Vergehen verfolgt, wobei dann häufig schon eine massive Störung aufgetreten sein muss, welche die öffentlichen Interessen stark berührt. Eine solche Störung könnte beispielsweise der Konkurs eines Unternehmens mit vielen Arbeitslosen als Folge sein, der durch einen Computerbetrug ausgelöst worden ist.

Der Staat gibt – beispielsweise in Deutschland und Österreich – immer häufiger auch Richtlinien heraus, die für den öffentlichen Dienst verbindlich sind, für die Privatwirtschaft jedoch den Status von Best Practice Verfahren haben und daher immer stärker angenommen werden. Beispielhaft sind hier das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Deutschland und das Österreichische IT-Sicherheitshandbuch der IKT-Stabstelle des Bundes genannt, die im Kapitel 4 noch näher erläutert werden.

Solche Best Practice Verfahren sind allerdings erst dann Anforderungen im Sinne des Security Managements, wenn das Unternehmen diese aktiv übernimmt, zum Beispiel in die übergeordneten Unternehmensziele (Corporate Policy).

Die Anforderungen aus der Gesellschaft werden häufig durch nicht-staatliche Organisationen gestellt, beispielsweise Normierungs- und Akkreditierungsinstitute, Standesvereinigungen (GI, VDI), Gewerkschaften oder organisierte Interessensgruppen (Greenpeace im Umweltbereich).

Im Gegensatz zu staatlichen Anforderungen sind diese Anforderungen freiwillig gewählt oder innerhalb von Branchen gemeinschaftlich beschlossen und ausgehandelt worden.

Der Markt, also die Gruppe aller potentiellen Kunden, Lieferanten und Wettbewerber hat de facto einen sehr starken Einfluss auf die Anforderungen. Besonders das Thema Sicherheit hat immer wieder Marktparadigmen verändert, wie beispielsweise den weltweiten Automobilmarkt.

In den 60er Jahren waren viele Neuwagen bereits bei der Auslieferung fehlerhaft, und zahlreiche tödliche Unfälle waren die Folge.

1965 veröffentlichte Ralph Nader, später der Begründer der Grünen Partei in den USA, das Buch „Unsafe at any Speed“[4], in dem er die Versäumnisse hauptsächlich der US-amerikanischen Automobilindustrie aufzeigte. Die Reaktionen der Automobilindustrie waren zunächst verhalten und halbherzig. Erst nachdem Nader nachweisen konnte, dass die Hersteller längst bekannte und nachweislich wirkungsvolle Sicherheitstechnik, wie zum Beispiel den Sicherheitsgurt, vorsätzlich nicht in die Fahrzeuge eingebaut

[4] Deutsch: „Unsicher bei jeder Geschwindigkeit“, Das Buch ist nur auf Englisch erschienen, aber seit vielen Jahren vergriffen.

hatten, begann ein Boykott dieser Marken durch die Käufer und damit ein bespielloser Wettlauf der Hersteller, ihre Modelle sicher zu machen. Sicherheitsgurte, bessere Bremsen, neue Lenkungssysteme und weiteres zählte in kürzester Zeit zur Standardausstattung. Autos ohne diese Merkmale waren nicht mehr verkäuflich. Damit wurde Sicherheit zum zentralen Kaufargument für Autos. Heute kann man sich Autos ohne Airbags, Gurtstraffer und Sicherheitsglas nicht mehr vorstellen.

Eine ähnliche Erfolgsgeschichte für die Sicherheit ist die Gründung des TÜV.

Die Maschinen, welche die Umstände, unter denen Menschen damals gearbeitet haben aus heutiger Sicht grundlegend revolutioniert haben, sind Ende des 18. Jahrhunderts auf den Markt gekommen, die Dampfmaschinen.

Dampfmaschinen bildeten die Motoren der Industrialisierung, indem sie die Herzstücke der Fabriken bildeten. Durch schlechte Verarbeitung, mangelnde Wartung und falsche Bedienung explodierten viele Dampfkessel, und hauptsächlich Kinder starben, da diese damals ungelernte und damit billige Arbeitskräfte waren.

Um drohenden Gesetzen zur stärkeren Reglementierung von Dampfkesseln zu entgehen, gründeten die Hersteller dieser Technik Dampfkessel Überwachungsvereine, Vorläufer des TÜV.

Heute stellen der TÜV und andere Organisationen sicher, dass zum Beispiel Industrieanlagen, Energieversorgungsinfrastrukturen, Schiffe und Autos bestimmte Qualitätsmerkmale erfüllen.

Diese Beispiele aus der Industrie haben jeweils massive Fehler mit starken gesellschaftlichen Auswirkungen gebraucht, um Sicherheit als notwendige und zentrale Forderung dauerhaft zu implementieren. Für die IT ist die Schlussfolgerung zu ziehen, dass anscheinend nicht genug passiert ist um einen gesellschaftlichen Druck auf Hersteller und Dienstleister zu erzeugen. Aktuelle Bedrohungen, wie digitaler Diebstahl von Bankenzugangsdaten und daraus folgender elektronischer Raub, könnten der Gesellschaft die tatsächliche Bedrohungslage vor Augen führen.

Jedes Unternehmen hat eigene Anforderungen, die für die IS betrachtet werden müssen. Diese sind bedingt durch viele Faktoren, wie Standort, Geschäftsprozesse, IT Services, Projekte, Unternehmensleitbilder und Mitarbeiter.

Es gibt vier Gliederungsebenen, auf denen die Anforderungen an die IS definiert werden:

1. Definition der übergeordneten Sicherheitsziele und Rahmenparameter (IS-Policy)
2. Definition was getan werden muss, um die Sicherheitsziele zu erreichen (Prozesse)
3. Definition wer was wann tun muss (Maßnahmen)
4. Festlegung von konkreten Arbeitspaketen (Arbeitsanweisungen).

Die Policy muss durch die Unternehmensleitung festgelegt werden. Hierbei sollte eine aktive Rolle der Unternehmensleitung bei der Gestaltung der Policy angestrebt werden, damit die Unternehmensziele optimale Berücksichtigung finden und die Unternehmensleitung die Policy auch zu 100% trägt. Die in vielen Projekten anzutreffende Variante, dass ein externer Berater die IS-Policy auf Basis seiner Erfahrung formuliert und der Unternehmensleitung nur zur Unterschrift vorlegt, führt spätestens dann zu kritischen Situationen, wenn andere Prozesse einen Zielkonflikt mit der IS haben. Ein typischer Zielkonflikt tritt beispielweise auf, wenn eine neue Intranet-Anwendung vom Security Manager als unzureichend sicher eingestuft wird, und somit die notwendige Freigabe nicht erteilt wird, der Fachbereich diese Anwendung aber um jeden Preis sofort implementieren will, weil eine wichtige Verbrauchermesse vor der Tür steht. Häufig fällt in solchen Situationen die Entscheidung für die Implementierung, wenn die Unternehmensleitung die Notwendigkeit und den Nutzen von IS nicht vollständig erkannt hat.

2.3 Maßnahmen

Die Sicherheitsziele können nur dann erreicht werden, wenn zuverlässige und angemessen Maßnahmen diese unterstützen. Es gibt vier Arten von Maßnahmen, die getroffen werden können:

- Organisatorische Maßnahmen der IS sorgen dafür, dass die Einbindung der Prozesse in die Unternehmensorganisation erfolgt, jeder seine Aufgaben kennt, die richtigen Verfahren gültig sind und diese ständig auf Einhaltung überwacht werden. Diese Art von Maßnahmen stellt den eigentlichen Kern des Security Management Prozesses dar.
- Physische Maßnahmen tragen beispielsweise dafür Sorge, dass Türen und Schränke verschlossen sind und der Zutritt zu sensiblen Bereichen, wie zum Beispiel dem Rechenzentrum, nur befugten Personen gestattet wird. Diese Art von Maßnahmen wird seit jeher von Unternehmen adressiert, weshalb Security begrifflich auch heute noch häufig mit diesen physischen Maßnahmen gleichgesetzt wird.
- Technologische Maßnahmen stellen die gesamte Bandbreite dar, wie Hard- und Software genutzt werden kann, um Informationen gegen die eine oder andere Bedrohung zu schützen, oder deren Auswirkung zu vermindern. Da diese Art der Maßnahmen im englischen Technical Measures heißt, dieser Begriff im deutschen aber nicht eindeutig belegt ist, werden diese nachfolgend kurz IS-Maßnahmen genannt.
- Verfahren sind die vierte und letzte Art der Maßnahmen. Ähnlich wie die organisatorischen Maßnahmen, die den Gesamtprozess betrachten, beschreiben Verfahren dedizierte Lösungen für einzelne Fragestellungen, beispielsweise wie ein Passwort genau auszusehen hat.

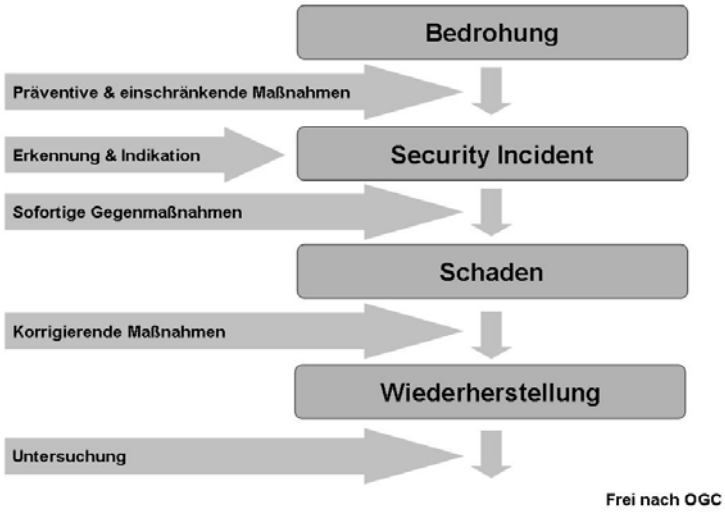


Abbildung 1: Wann werden Maßnahmen gebraucht

Die unterschiedlichen Arten von Maßnahmen helfen an unterschiedlichen Stellen, die Sicherheitsziele zu erreichen:

- Präventive Maßnahmen (engl. Prevention) verhindern das Eintreten von Security Incidents. Ein Beispiel für eine präventive Maßnahme ist die Deaktivierung sämtlicher USB-Anschlüsse an einem Arbeitsplatz-PC, so dass die Bedrohung des Datendiebstahls durch Nutzung mobiler Speichergeräte verhindert werden kann.
- Wo man eine Bedrohung nicht von vornherein ausschließen kann, werden einschränkende Maßnahmen (engl. Reduction) ausgewählt, welche die Eintrittswahrscheinlichkeit oder die Schadensauswirkung reduzieren. Ein adäquater Notfallplan stellt eine solche Maßnahme dar, da dieser die Ausfallzeit und damit den Schaden mindert.

- Maßnahmen zur Erkennung (engl. Detection) sollten so schnell wie möglich einen Security Incident entdecken. Dieses ist jedoch schwierig, da sich häufig erst nach einer genauen Analyse und damit auch erst nach einer gewissen Zeit herausstellt, ob es sich bei einer Störung um einen Security Incident handelt oder nicht. Daher werden hier nicht nur Maßnahmen ausgewählt, die ein tatsächliches Erkennen durchführen, sondern auch solche Maßnahmen (engl. Indication), die brauchbare Indikatoren darüber liefern, dass es sich wahrscheinlich um einen Security Incident handelt. Die Maßnahmen für Erkennung und Indikation sind häufig die gleichen, wie zum Beispiel bei Anti-MalWare, die bekannte MalWare gegen ein eindeutiges Muster (engl. Pattern) vergleicht und somit das Auftreten von MalWare, also einem Security Incident, erkennt. Dieselbe Software sucht aber auch nach Indikatoren, die nur auf ein Auftreten von MalWare hinweisen, beispielsweise durch heuristische Verfahren oder durch Analyse der Abläufe (engl. behaviour indication). In jedem Fall wird eine Erkennung angezeigt.
- Wenn ein Security Incident geschehen ist, sorgen Gegenmaßnahmen (Repression) dafür, dass dieser Security Incident nicht sein vollständiges Schadenspotential entfalten kann. So können beispielsweise Benutzerpasswörter gesperrt werden, wenn diese mehrmals falsch eingegeben worden sind, wobei die mehrfache falsche Eingabe ein Security Incident ist und die mögliche Bedrohung ein Zugriffsversuch durch einen Unbefugten.
- Nachdem ein Schaden eingetreten ist, beispielsweise der Verlust von Daten, sorgen korrigierende Maßnahmen (Correction) dafür, dass der eingetretene Schaden sich nicht oder nicht so stark auf die Geschäftsprozesse und anderen Prozesse auswirkt. So kann eine korrigierende Maßnahme beim Datenverlust das Wiedereinspielen (engl. Restore) einer Sicherungskopie sein, aber ebenso gut eine Presseerklärung, dass Mails aus dem eigenen Unternehmen nicht geöffnet werden dürfen, da sich dort MalWare eingeschlichen hat.
- In jedem Falle sollten Maßnahmen zur Untersuchung von Security Incidents durchgeführt werden, um herauszufinden, was genau passiert ist, und um Anpassungsbedarf von Maßnahmen zu identifizieren. Regelmäßige Audits prüfen darüber hinaus, ob Security Incidents aufgetreten sind, die noch nicht erkannt worden sind.

2.4 Der Security Management Prozess

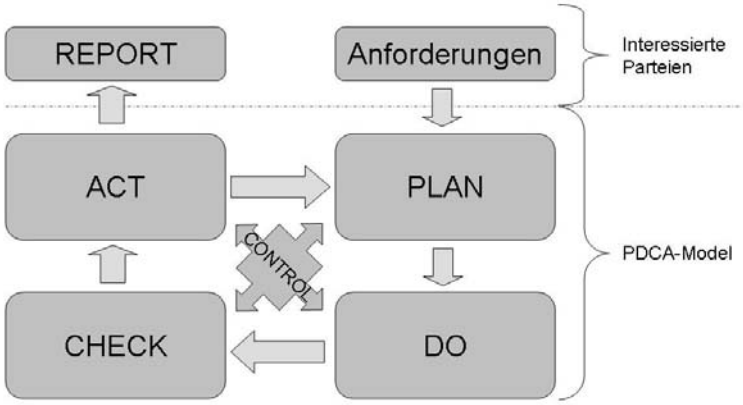


Abbildung 2: Security Management Prozess

ITIL definiert den Security Management Prozess wie in Abbildung 2 analog zur ISO/IEC 17799, einer international gültigen Verfahrensregel (engl. Code of Practice) zum Aufbau und Betrieb von IS Management Systemen (ISMS).

Dieser Prozess basiert auf dem PDCA-Modell (Plan-Do-Check-Act) von W.E. Deming, dem meistbenutzten Ansatz für einen Prozesskreislauf, der sich ständig überprüft und optimiert. In diesem Prozesskreislauf werden die Aktivitäten des Security Management im Zusammenhang mit den interessierten Parteien betrachtet. Dieses sind diejenigen, die Anforderungen stellen oder Erwartungen haben, also Staat, Gesellschaft, Markt und Unternehmen.

ANFORDERUNGEN

Die Anforderungen werden bereits außerhalb des Security Management Prozesses gestellt, müssen dort jedoch zusammengetragen und bewertet werden. Bei ITIL sind diese Anforderungen als Sicherheitsziele in einer Vereinbarung über den Umfang und die Qualität der IT-Services (Service Level Agreement, SLA) definiert. Dieses wird später im Kapitel über das Service Level Management detailliert beschrieben.

CONTROL

Das PDCA-Modell wird ergänzt um eine Control-Phase, die den Prozess im eigentlichen Sinne kompatibel gemäß ITIL gestaltet.

Die Control-Phase ist verantwortlich für das Security Management Rahmenwerk:

- Definition von Security Plänen
- Implementierungsrichtlinien
- Prüfungsrichtlinien
- Verbesserungswesen
- Berichtswesen
- Definition der Security Organisation, inklusive
  - Rollen
  - Verantwortlichkeit
  - Eskalation.

Ein Prozess benötigt einen Startpunkt (Input) und liefert ein Ergebnis (Output). Häufig stellt der Output eines Prozesses den Input für einen weiteren Prozess dar. Die Control-Phase regelt die Organisation des Security Management Prozesses, so dass es eine nahtlose Verbindung zu den anderen ITIL Prozessen gibt.

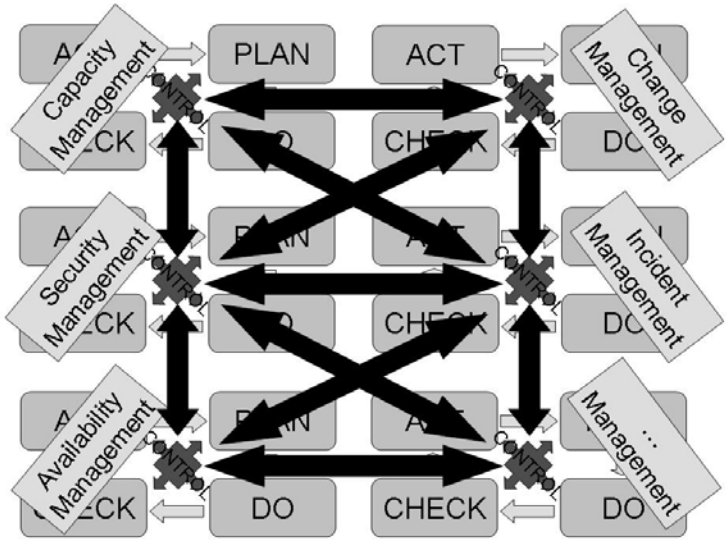


Abbildung 3: Verbindung zwischen Prozessen

Verantwortlich für den Security Management Prozess ist der Security Manager, der die direkte Schnittstelle zu den Verantwortlichen der anderen Prozesse darstellt. Der Security Manager kann eine Rolle oder eine Funktion sein, wobei zu beachten ist, dass die Trennung der Verantwortlichkeit (engl. Segregation of Duties) eingehalten wird, und ein Security Manager sich nicht selbst beispielsweise in der Funktion „System Administrator“ überprüfen soll.

Der Security Manager bewegt sich in einem hohen Spannungsfeld zwischen den Sicherheitszielen, den implementierten Maßnahmen und den Anwendern. Nur wenn Anwender die Maßnahmen annehmen, können die Sicherheitsziele erreicht werden.

Der Auswahl des Security Managers kommt daher eine große Bedeutung zu. Jedes Unternehmen hat eine andere Kommunikations- und Unternehmenskultur, daher kann kein Patentrezept für die Auswahl des optimalen Security Managers gegeben werden. Einige Fähigkeiten und Eigenschaften sollte ein Security Manager jedoch grundsätzlich mitbringen, um in dem Spannungsfeld zu bestehen.

Die erste häufig gestellte Frage ist, welche Position ein Security Manager in einer Hierarchie übernehmen sollte. Dies hängt im hohen Maße von der betroffenen Person ab und deren persönlichem Werdegang. Es gibt aber drei Positionen, auf denen Security Manager meistens etabliert werden.

1. Security Manager werden sehr häufig in Stabstellen organisiert. Das liegt einerseits daran, dass dieses eine gängige Position für Datenschutzbeauftragte ist, die nicht selten auch die Funktion des Security Managers übernehmen. Die Position spiegelt aber auch das klassische Verständnis dieser Rolle wieder. Nahe am Vorstand sorgt der Security Manager für ein hohes Maß an Transparenz und Informationsfluss gegenüber der Unternehmensleitung - manchmal aber auch für ein ruhiges Gewissen bei der Unternehmensleitung, dass alles für die IS getan worden ist.

   Eine Stabstelle hat, wenn diese richtig implementiert ist, eine gute Chance, das Thema IS unternehmensweit voranzubringen. Meist geht diese Position jedoch damit einher, dass der direkte Kontakt mit den operativen Ein-

heiten verloren geht. In einer Stabstelle kann ein Security Manager nur dann erfolgreich sein, wenn er ein erfahrener Manager ist, der auch Konflikte mit der Unternehmensleitung nicht scheut.

2. Wenn der Security Manager eine Führungskraft ist (Bereichs-, Abteilungs- oder Referatsleiter), hat er neben der Richtlinienkompetenz kraft seines Amtes auch eine Position, die ihn befähigt, die Richtung mitzugestalten, in die das Unternehmen geht. Wichtig ist der Zuschnitt des Bereiches oder der Abteilung, dem diese Führungskraft vorsteht, um hier frühzeitig Zielkonflikte zu vermeiden. Beispielsweise ist es problematisch, wenn der Abteilungsleiter der Abteilung Netzwerke gleichzeitig Security Manager ist, da er dann seine eigene Arbeit und die seiner Mitarbeitern überwachen soll. Ein großer Vorteil der Konstellation Führungskraft als Security Manager sind die Weisungskompetenz und das Agieren auf der Unternehmensebene, in der die Entscheidungen getroffen werden. Gerade in dieser Konstellation muss ein Manager diese Rolle mit Instinkt und Standfestigkeit ausfüllen, da er im Zweifelsfalle, wenn es um die Erreichung der Sicherheitsziele geht, die anderen Führungskräfte anweisen und führen muss.

3. Manchmal wird auch ein IT-Experte zum Security Manager bestellt. Meist nimmt er bereits eine zentrale Rolle im operativen Security Management wahr, zum Beispiel die Administration der Firewall oder der Anti-MalWare.

   In diesem Fall schlägt ein hohes Spezial-Knowhow zu Buche, wodurch der Security Manager im Zweifelsfall vollständig autark entscheiden kann, welche Aktivitäten zu treffen sind, um die Sicherheitsziele optimal zu unterstützen. Dieses sehr tiefe Wissen in einem Bereich bedeutet aber häufig auch ein schlechteres Verständnis von anderen Bereichen. Ein ausgeprägter Generalismus ist jedoch für den Security Manager genauso wichtig wie ausgeprägtes Interesse und Durchsetzungsfähigkeit. Daher sollten Mitarbeiter mit einem zu hohen Spezialisierungsgrad nicht der Kopf einer Security Management Organisation sein. Dazu ist es problematisch, wenn die Führungskräfte im Zweifelsfalle von einem IT-Mitarbeiter angewiesen werden.

Generell gilt, dass ein Security Manager ein guter Kommunikator sein sollte, der bis in die Unternehmensleitung akzeptiert wird. Er muss entscheidungsfähig sein und darf auch unbequemen Fragen nicht aus dem Weg gehen.

Darüber hinaus sollte er eine langjährige Erfahrung im IT-Umfeld, möglichst in der IS haben und sich mit dem Aufbau und der Implementierung von Prozessen auskennen.

Häufig sind gestandene Projektmanager gute Security Manager, da für ein Projekt die Risikoeinschätzung von zentraler Bedeutung ist.

Für die Geschäftsprozesse des Unternehmens sollte der Security Manager ein gutes Verständnis haben. Er muss kein ausgewiesener Fachspezialist sein, sollte sich aber schnell in Themen einarbeiten können.

PLAN

Die Plan-Phase ist dafür verantwortlich, dass die Sicherheitsziele, so wie diese im SLA vereinbart worden sind, in operationale Ziele heruntergebrochen werden und Vereinbarungen zur Leistungserbringung (Operational Service Agreement, OLA) mit den ausführenden Einheiten abgeschlossen werden.

Weiterhin muss hier eine IS-Policy erstellt werden, aus der die Ziele und der Umfang des ISMS hervorgehen.

In den OLAs sind die Maßnahmen beschrieben, die getroffen werden müssen, um die Sicherheitsziele zu erreichen. Diese Maßnahmen müssen auf Basis einer risikobasierten Vorgehensweise ausgewählt werden. Dazu muss eine Risikoanalyse durchgeführt werden.

Im besten Fall ist ein Risikomanagement bereits implementiert, so dass eine Methode zur Risikobewertung etabliert ist. Wenn allerdings ein Risikomanagement nicht implementiert ist, oder sich dieses nicht mit operativen IS-Risiken beschäftigt, muss hier ein Ansatz zur Risikobewertung gewählt und in der IS-Policy verbindlich festgeschrieben werden. Nur so können Risiken über den gesamten Lebenszyklus von IT-Services vergleichbar gemacht werden.

Die Vergleichbarkeit ist von großer Relevanz in Bezug auf Aussagen zur Risikoentwicklung und zur Auswahl wirtschaftlich sinnvoller Gegenmaßnahmen.

Die Beschreibung der Maßnahmen in den OLAs stellen die Security Pläne dar.

DO

Die Do-Phase ist für die Implementierung und den Betrieb der IS-Policy, Prozesse und Maßnahmen verantwortlich. ITIL referenziert hier den ISO/IEC 17799 Code of Practice, wobei andere Standards und Richtlinien ebenso als Referenz genommen werden können, wie beispielsweise das BSI Grundschutzhandbuch.

Die Do-Phase wird im Kapitel 5 detaillierter betrachtet.

CHECK

Die Check-Phase ist die Qualitätssicherungskomponente im PDCA-Model, die sicherstellt, dass die Maßnahmen auch tatsächlich die Sicherheitsziele erreichen. Sie führt Prüfungen durch, mit den Zielen, unabhängig und transparent

- die Effektivität der Maßnahmen zu ermitteln,
- internes und externes Vertrauen in die IS zu erzeugen,
- Optimierungspotentiale zu identifizieren und
- Security Incidents zu finden.

Dabei gibt es drei Hauptprüfarten zur Qualitätssicherung:

1. Durch Prüfungen (Review) von Dokumenten und Maßnahmen werden die bestehenden Dokumente und Maßnahmen regelmäßig oder stichprobenartig dahingehend untersucht, ob die beschriebenen Abläufe die Sicherheitsziele noch adäquat unterstützen. Andererseits werden neue Verfahren und IT-Services untersucht, um im Vorfeld eine starke Einbindung der bestehenden Maßnahmen zu erreichen und die Sicherheitsziele so frühzeitig abzusichern.
2. In Interviews oder Workshops wird die strategische und taktische IS untersucht. Interviews und Workshops sind abgeschwächte Formen der nächsten Stufe, nämlich der Audits. Meistens sind die Verantwortlichen in den strategischen und taktischen Bereichen in höheren Führungsebenen aufgestellt, die das operative Tagesgeschäft nicht direkt verantworten, dieses aber über die Zielsetzung steuern. Daher werden hier

hauptsächlich die Verfahren der Zielermittlung und –kommunikation sowie der Unterstützung dessen durch ein entsprechendes Berichtswesen untersucht. Bei Workshops kann zudem noch ein größerer Kreis mit in den Prüfungsprozess einbezogen werden. Häufig werden so durch Workshops mit wenig Aufwand sehr gute Ergebnisse erreicht.

3. Die häufigste und facettenreichste Form der Prüfung ist das Audit. In dieser werden Maßnahmen und Arbeitsabläufe auf ausreichende Beweise dafür untersucht, ob Maßnahmen eingehalten worden sind und erfolgreich waren. Häufig wird vom Auditierten beispielsweise ein Nachweis dafür verlangt, dass ein Verfahren zur Einrichtung eines Anwenders eingehalten worden ist, also dieser hinsichtlich seiner Pflichten informiert worden ist, ihm erklärt wurde, wie er ein sicheres Passwort erzeugen kann und was er tun muss, wenn er eine verdächtige E-Mail erhält. Gültige Beweise wären hier beispielsweise eine durch den Anwender abgezeichnete Erklärung oder eine Statistik zur Einhaltung der Passwort-Regeln. Audits können aber auch technische Untersuchungen sein, welche die Prüfung von Systemen, Netzwerken und Software-Anwendungen zum Ziel haben.

Es gibt darüber hinaus noch zahlreiche andere Prüfungsarten, die sich aber alle auf die drei oben aufgelisteten Arten abbilden lassen, zum Beispiel das Social Engineering, also die Überprüfung, ob von internen Anwendern Auskünfte erlangt werden können, die gegen Sicherheitsziele verstoßen, beispielsweise die Weitergabe eines Passwortes.

Weiterhin gibt es drei Prüfaspekte, die jeweils aus der Sicht des Prüfers betrachtet werden:

Der mildeste Aspekt ist die Selbstauskunft, das so genannte Self Assessment. Hier bewertet sich eine Organisationseinheit selbst mit Hilfe von vordefinierten Fragen. Diese Selbstauskunft eignet sich besonders gut für eine Standortbestimmung sowie dazu, die Problematik der IS innerhalb von Organisationseinheiten zu thematisieren. Da die selbstkritische Komponente häufig durch politische und hierarchische Fragen überlagert wird, sollte dieses Verfahren durch den Security Manager begleitet oder moderiert

werden. Es muss allerdings die Aufgabe der Organisationseinheit bleiben sich zu bewerten, und darf nicht als Dienstleistung komplett an den Security Manager übertragen werden. Self Assessments dienen dem Security Management später dazu, Schulungsbedarf zu ermitteln und besondere Prüfungen zu identifizieren.

Die interne Prüfung wird häufig durch die Innen- oder IT-Revision durchgeführt oder durch den Security Manager selbst. Während die Innen- und IT-Revision das Prüfziel hat festzustellen, ob dem Unternehmen mittels IT-Services oder Systemen Schaden zugefügt worden ist, sei es finanzieller oder anderer Natur, prüft der Security Manager, inwieweit die Sicherheitsziele selbst eingehalten worden sind, beziehungsweise wie diese besser erreicht werden können. Die Betrugsaufklärung ist nicht Aufgabe des Security Managers, wenngleich er zur Amtshilfe durch die Revision hinzugenommen werden kann.

Als dritten Aspekt gibt es die Prüfung durch externe Prüfer, wobei sich hier die Motivation erheblich unterscheiden kann. Bei Prüfungen im Auftrag des Unternehmens wird häufig externer Expertenrat gesucht, um entweder die Unabhängigkeit zu manifestieren, oder Knowhow zu nutzen, das im Unternehmen nicht verfügbar ist. Eine Prüfung im Auftrag des Unternehmens ist aber auch eine bestellte Wirtschaftsprüfung, die immer stärker auch die IS fokussiert. Diese externen Prüfer müssen durch das Security Management unterstützt werden, wobei das Security Management ebenfalls auf die Einhaltung der festgelegten Maßnahmen durch diese externen Prüfer zu achten hat.

Prüfungen im Auftrag anderer Unternehmen stehen häufig unter einem anderen Vorzeichen, zum Beispiel einer Due Diligence oder einem Rating, wie es zunehmend für die Bewertung von Risiken für Kreditvergabe durchgeführt wird. Das Vorhandensein eines ISMS und speziell der Notfallplanung, aber auch das Vorhandensein eines Qualitätsmanagements und die Ausrichtung auf Prozesse überhaupt sind dabei wesentliche Prüfpunkte.

Externe Prüfungen können auch zum Zweck der Zertifizierung durchgeführt werden. Die Aufgabe des Security Managements bei solchen externen Prüfungen ist die Aufrechterhaltung der IS-Maßnahmen. Er muss beispielsweise sicherstellen, dass externe Prüfer nicht mit ihren Notebooks auf das Unternehmensnetzwerk zugreifen können.

Eine besondere Prüfung ist die Prüfung durch die Finanzbehörden gemäß den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Diese sind keine Prüfungen im Sinne der IS, sondern stellen mögliche Security Incidents dar, wenn nämlich durch einen Prüfer der Finanzbehörde unbefugte Informationen erlangt werden. Daher ist es wichtig, dass durch das Security Management gemeinsam mit den entsprechenden Fachbereichen ein Verfahren entwickelt wird, wie den Anforderungen gemäß GDPdU entsprochen werden kann und gleichzeitig die Sicherheitsziele eingehalten werden können.

In Bezug auf die Check-Phase ist wichtig, dass die Erkenntnisse aus den Prüfungen dazu führen, die IS-Maßnahmen und Verfahren zu optimieren, um die Sicherheitsziele auf effektive und effiziente Art sicherzustellen.

ACT

Die Act-Phase stellt sicher, dass gefundene Schwachstellen abgestellt, Optimierungspotentiale genutzt und Maßnahmen eingehalten werden.

Ziel ist es, den erreichten Grad der IS zu halten und sogar noch zu steigern. Dieses wird erreicht, indem alle Änderungen auf die Frage hin analysiert werden, wie diese sich auf die IS auswirken, sowie durch eine regelmäßige Risikobewertung und daraus resultierende Anpassungen der Maßnahmen.

Diese vier Kernaktivitäten des PDCA-Modells bilden einen iterativen Prozess, der einen dauerhaften Kreislauf beschreibt und sich somit permanent überprüft und verbessert.

REPORT

Die Report-Phase gehört nicht mehr in das ursprüngliche PDCA-Model. Während im klassischen PDCA-Model das interne Berichtswesen in jeder Phase durchgeführt wird, muss beim Security Management nach ITIL ein externes Berichtswesen implementiert werden, da die Anforderungen ebenfalls von außen gekommen sind. Dieses externe Berichtswesen wird durch die Report-Phase wahrgenommen.

Darüber hinaus ist es für das Security Management von vitaler Bedeutung die Ergebnisse und den Status der IS Dritten, zum Beispiel der Unternehmensleitung, zu vermitteln, denn die IS ge-

hört zu den Dingen, über die häufig ein Mantel des Schweigens gebreitet wird, frei nach dem Motto: „Keine Nachrichten sind die besten Nachrichten“.

Manchmal wird auch die IS selbst bemüht, kein Berichtswesen aufzubauen, gemäß dem Prinzip „Sicherheit durch Verschleierung“ (engl. Security by Obscurity). Im Extremfall wird hier sogar das Vorhandensein eines Security Managements verschwiegen.

Wenn aber keine Informationen über die Wirksamkeit von Verfahren und IS-Maßnahmen oder aktuelle Bedrohungen berichtet werden, geht es dem Security Management wie vielen anderen Feigenblatt-Aktivitäten: Man muss es machen, aber bitte nur das Offensichtlichste!

Ohne ein vernünftiges Berichtswesen wird die IS und damit das Security Management niemals als Motor gesehen, der Chancen bietet und Türen aufmacht.

Durch Auswahl der geeigneten Kennzahlen bietet das Berichtswesen der Unternehmensleitung zudem die Möglichkeit Trends frühzeitig zu erkennen und gegenzusteuern.

2.5 Security Management im Kontext anderer IT Prozesse

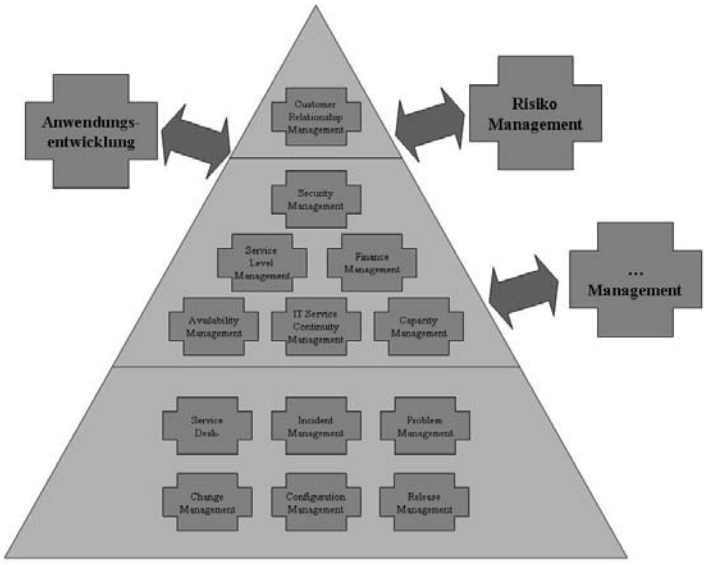


Abbildung 4: Security Management im Kontext

Das Security Management steht in einem regen Austausch mit anderen IT-Prozessen. Die IT-Betriebsprozesse der taktischen und operativen Ebene, wie im ITIL beschrieben, werden im Kapitel 3 Security Management und ITIL detailliert beschrieben. Eine sinnvolle Schnittstelle besteht auch zu dem Entwicklungsprozess, da das Thema „Designed for Security“ in der Anwendungsentwicklung einen immer stärkeren Stellenwert erlangt. Eine weitere sinnvolle Schnittstelle besteht zum Qualitätsmanagement von Software-Anwendungen, da IS als nicht-funktionales Qualitätsmerkmal auch hier eine immer größere Bedeutung erhält.

Da diese Bereiche aber derzeit nicht so sehr im Fokus von ITIL stehen, werden sie hier nicht näher betrachtet.

Eine weitere wichtige Schnittstelle ist die zum Risiko Management, da durch das Security Management Risikoanalysen durchgeführt werden müssen.

- In einer Risikoanalyse werden Betriebsmittel (Assets) dahingehend untersucht, ob für diese Bedrohungen existieren und ob Schwachstellen diese Bedrohung fördern.

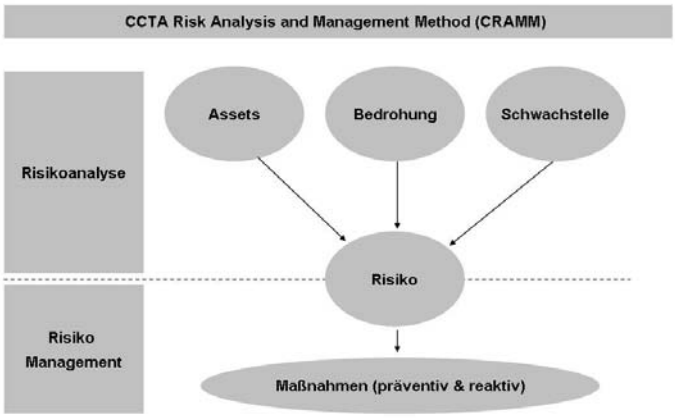


Abbildung 5: Risikoanalyse gemäß CCTA

Nur wenn das Risiko und die Auswirkung auf einen Geschäftsprozess bekannt sind, können angemessene Maßnahmen ergriffen werden.

Häufig bewerben sich unterschiedliche Maßnahmen um enge Budgets, und nur ein risikobasierter Ansatz kann die richtigen Maßnahmen identifizieren, um die Sicherheitsziele optimal zu unterstützen.

2.6 Kritische Erfolgsfaktoren

- Die Unternehmensleitung muss das Security Management 100%ig unterstützen. Dazu ist es notwendig, dass es eine aktive Rolle erhält, indem es die Sicherheitsziele definiert und durch ein aussagekräftiges Berichtswesen die tatsächliche Leistungsfähigkeit beurteilen kann.
- Es gibt einige zentrale Prozesse, die implementiert sein sollten, um einen erfolgreichen Security Management Prozess aufzubauen. Diese Prozesse sind das Change Management und das Incident Management.
- Ein Prozessualer Ansatz sollte bereits im Unternehmen vorhanden sein.
- Für ein erfolgreiches Security Management ist eine Unternehmenskultur förderlich, die Prüfungen nicht als Verhaltenkontrolle versteht, sondern offen mit Schwachstellen und Fehlern umgeht. Denn nur durch permanente Prüfung und Verbesserung kann eine solide Basis geschaffen werden.

2.7 Stolpersteine

Die größten Stolpersteine des Security Managements liegen in der Planung und Implementierung des Prozesses. Sobald der Prozess erst einmal eingeführt und akzeptiert worden ist, werden durch die Check- und Act-Phasen mögliche Abweichungen identifiziert und können abgestellt werden. Bei dem Aufsetzen der Organisation während der Control-Phase jedoch treten die meisten Schwierigkeiten auf.

Manchmal wird versucht, die Aufgaben eines Security Management Prozesses durch ein Werkzeug (Tool) vollständig zu ersetzen. Hier wird von dem Ansatz ausgegangen, dass die Funktionalitäten eines Tools analog zu den Aufgaben eines Prozesses zu sehen sind, und ein Prozess daher nicht benötigt wird. Ein erfolgreicher Security Management Prozess beschreibt jedoch innerhalb des Prozesses die notwendigen Maßnahmen, die benötigt werden, um die Sicherheitsziele zu erreichen. Ein Tool kann immer nur eine Maßnahme sein, die verwaltet werden muss.

Merke „A fool with a tool is still a fool".

Fehlende Rückendeckung durch die Unternehmensleitung führt schnell dazu, dass in Situationen, in denen Zielkonflikte zwischen Prozessen auftreten, das Security Management zurückgestellt wird. Diese fehlende Rückendeckung muss daher in einer Risikoanalyse untersucht werden, bevor der Security Management Prozess implementiert werden soll.

Ein nicht funktionierendes Change Management führt zu großen Problemen, da der Security Manager schnell den darüber Überblick verliert, welche Änderungen bereits durchgeführt worden und welche geplant sind. Die Planung von Maßnahmen benötigt aber das Wissen über die aktuelle Infrastruktur.

Die Motivation und das Wissen der Anwender ist sehr unterschiedlich. Wenn die Sicherheitsziele den Anwendern nicht nachdrücklich vermittelt werden können, wird die Erreichung dieser nicht möglich sein.

Häufig entsteht bei der Einführung eines Security Management Prozesses ein so genannter Grüne-Wiese-Effekt. Damit werden unterschiedliche Effekte beschrieben:

- Bereits eingeführte Verfahren werden nicht in den Prozess mit eingebaut, weil das Projekt „es gleich richtig machen möchte“ und nicht die Fehler der Vergangenheit weiterführen möchte.
- Durch Zeit und Budgetdruck erleben solche Projekte meist irgendwann eine Deckelung der Ressourcen, so dass neue und bessere Verfahren nicht mehr berücksichtigt werden können.
- Durch einen individuellen, aus der Erfahrung vieler Projekte, recht starren Rahmen können andere Verfahren nicht einfach angekoppelt werden, ohne die Integrität des gesamten Prozesses zu gefährden.
- Der Prozess, der zum Schluss eingeführt wird, hat keinen Wiedererkennungswert bei den Anwendern, so dass eine längere Implementierungsdauer notwendig wird oder der Prozess niemals erfolgreich arbeiten wird.

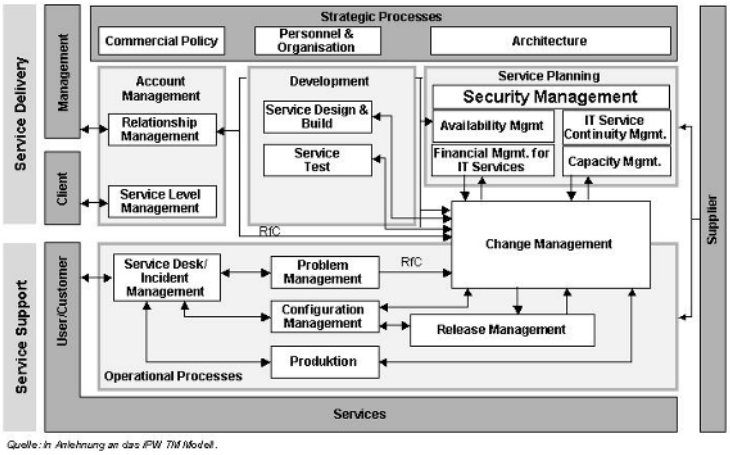
3 Security Management und ITIL

Im folgenden Kapitel soll eine Einordnung des Security Managements in ITIL vorgenommen werden. Dazu werden die am häufigsten genutzten Prozesse dahingehend untersucht, welche Schnittstellen zum Security Management bestehen.

3.1 Was ist ITIL?

Die Information Technology Infrastructure Library (ITIL) beschreibt die Prozesse, die IT-Dienstleister implementieren müssen, um IT-Services erfolgreich zu betreiben. IT-Dienstleister können sowohl interne IT-Abteilungen sein, wie auch externe Unternehmen, die IT-Dienstleistungen für Dritte erbringen. Im Mittelpunkt steht in jedem Falle die Ausrichtung aller IT-Services auf den Bedarf des Kunden. Bei internen IT-Abteilungen ist der Kunde dann ein Fachbereich, bei externen Dienstleistern ist der Kunde ein externes Unternehmen.

ITIL ist in fünf Hauptwerke gegliedert, wovon in diesem Buch zwei näher untersucht werden, und zwar der Service Support, sowie das Service Delivery, die jeweils auch die Grundlage für die Zertifikatslehrgänge bilden.



Quelle: In Anlehnung an das IPW TM Modell.

Abbildung 6: IPW Model

Der Herausgeber von ITIL ist das Office of Government Commerce (OGC), eine Abteilung des britischen Finanzministeriums.

Ziel von ITIL ist die Standardisierung der IT-Prozesse sowie deren Begriffe. Ohne eine solche Schablone herrschen oft babylonische Zustände, und es gibt unterschiedliche Meinungen darüber, welche Aufgaben beispielsweise das Configuration Management hat. In diesem Buch werden die englischen ITIL Begriffe benutzt, jedoch wird ihre Bedeutung jeweils erläutert.

Die größten Unterschiede in der Begrifflichkeit sind zwischen der IT-Entwicklung und dem IT-Betrieb auszumachen. Hier liegt derzeit noch eine große Baustelle von ITIL, da fast ausschließlich IT-Betriebsprozesse beleuchtet werden, aber ein Großteil der Budgets in die Entwicklung investiert wird. Das OGC hat in einem ITIL Refresh Statement angekündigt, zukünftig stärker auf die verschiedenen Lebensabschnitte von IT-Services einzugehen. Dieses wird die Lücke bei den Entwicklungsprozessen hoffentlich schließen und zu einer übergreifenden Begriffsdefinition führen.

Die Prozesse, die durch ITIL beschrieben werden, basieren auf Best Practice Ansätzen, also in der Praxis bewährten Prozessen.

Der Erfolg von ITIL liegt in der absoluten Praxistauglichkeit, die es jedem Unternehmen ermöglicht, für seinen Bedarf die optimalen Prozesse zu definieren und auch umzusetzen. ITIL ist kein Rahmenwerk, das Paperware, also nutzlose Konzepte produziert, sondern praktische Verfahren, die in der richtigen Reihenfolge umgesetzt, zu einer Erhöhung der Effizienz und Effektivität der IT-Services führen.

Der modulare Aufbau von ITIL führt in vielen Unternehmen dazu, dass im Umfang begrenzte Projekte, in denen einzelne Prozesse eingeführt worden sind, zu einer Keimzelle der ITILisierung geführt haben, quasi als Proof-of-Concept der Idee hinter ITIL.

Weitere Pluspunkte sind die nicht proprietäre und nicht an bestimmte Branchen gebundene Gültigkeit von ITIL sowie die starke Unterstützung durch die ITIL Gemeinschaft, die durch das IT Service Management Forum® (itSMF) jedem Interessierten eine breite Informationsbasis bietet und einen lebendigen Austausch fördert. Ein großes Beratungs- und Schulungsangebot sorgen für eine immer stärkere Verbreitung von ITIL.

Leider hat ITIL keine eindeutige Versionierung, so dass derzeit unterschiedliche Begriffe im Umlauf sind. Einerseits hängt es immer von der zitierten Quelle ab, andererseits ist es selbst für ITIL Kenner nicht immer einfach festzustellen, welche Begriffe nun die aktuellen und damit „richtigen“ Begriffe sind.

Selbst offizielle und aktuelle ITIL Bücher nutzen unterschiedliche Terminologien.

Aus diesem Grunde werden in diesem Buch die Begriffe benutzt, die auch für die ITIL Foundation Level Prüfung Gültigkeit haben. In den jeweiligen Kapiteln wird auf weitere Begriffe und Terminologien hingewiesen, so dass ein roter Faden mit anderer deutschsprachiger ITIL Literatur sichtbar bleibt.

3.2 Prozessreife

Um eine effiziente und effektive Bewertung des Reifegrades von Prozessen vornehmen zu können, wurde für ITIL ein einfaches Reifegradmodell entwickelt mit den folgenden Stufen:

Ebene 1: Vorbedingungen

Hier werden die Vorbedingungen abgefragt, die notwendig sind, um den Prozess erfolgreich zu implementieren.

Ebene 1.5: Unternehmensausrichtung

Hier wird die Ausrichtung und Zielsetzung des Unternehmens in Bezug auf das Security Management untersucht.

Ebene 2: Prozesstauglichkeit

Hier wird die Tauglichkeit des Unternehmens untersucht, einen Security Management Prozess zu implementieren, indem bereits implementierte Verfahren ermittelt werden.

Ebene 2.5: Interne Integration

In dieser Ebene wird untersucht, ob die Aktivitäten ausreichend miteinander verbunden sind, um einen durchgängigen Prozess zu gewährleisten.

Ebene 3: Ergebnisse

In dieser Ebene wird untersucht, ob die benötigten Ergebnistypen definiert sind und die Ergebnisse, beispielsweise Berichte, erzeugt werden.

Ebene 3.5: Qualitätskontrolle

Während der Qualitätskontrolle werden die Ergebnisse dahingehend überprüft und analysiert, ob diese die erwartete Qualität erreicht haben.

Ebene 4: Berichtswesen

Das Berichtswesen wird benötigt für die Steuerung des Prozesses. Durch das Berichtswesen wird zudem sichergestellt, dass der Unternehmensleitung zur richtigen Zeit die richtigen Informationen vorliegen, um die richtigen Entscheidungen treffen zu können.

Ebene 4.5: Externe Integration

Die Externe Integration bedeutet, dass die einzelnen Prozesse miteinander so verbunden sind, dass diese die übergeordneten Unternehmensziele unterstützen.

Ebene 5: Schnittstelle zum Kunden

Die Schnittstelle zum Kunden soll sicherstellen, dass die Anforderungen durch den Kunden immer die Grundlage des Prozesses sind.

Im Anhang befindet sich ein Fragebogen, der für ein Self Assessment genutzt werden kann. Dieser Fragebogen ist nicht der offizielle Fragebogen des OGC oder des itSMF. Er wurde entwickelt auf Basis der oben beschriebenen Ebenen und soll dabei helfen, einen Überblick zu gewinnen, wie reif der Security Prozess schon ist.

3.3 Einordnung von Security in ITIL

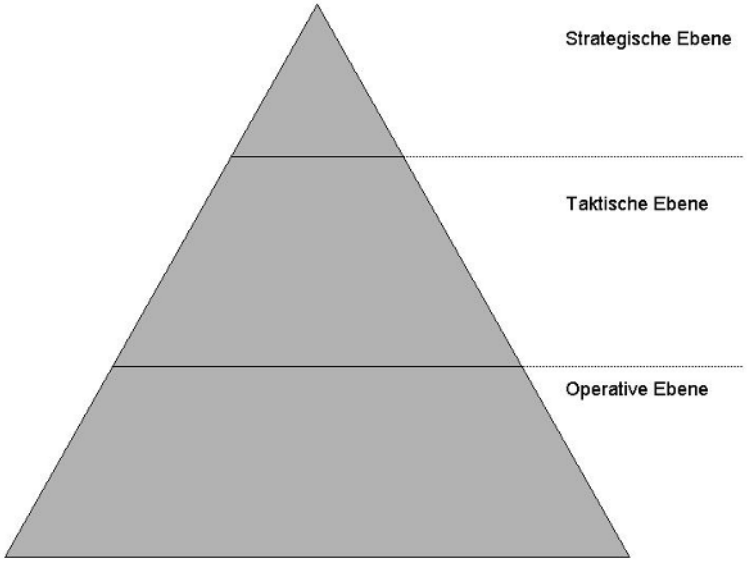


Abbildung 7: Die Ebenen von ITIL

Die Abbildung 7 stellt die Ebenen von ITIL dar.

Auf der obersten Ebene werden strategische Entscheidungen getroffen und somit die Arbeitsfähigkeit des Security Managements festgelegt. Hier wird entschieden, dass ein Security Management aufgebaut wird. Ebenfalls hier wird die Corporate Policy festgelegt, welche das Security Management steuert.

Die taktische Ebene besteht aus den Prozessen des Service Delivery. Das Service Delivery beinhaltet die Prozesse, die für die Planung und Steuerung der IT Services notwendig sind. Das Security Management ist ebenso ein Prozess im Service Delivery wie das Service Level Management, das die Anforderungen festschreibt und damit die Ziele der Informationssicherheit definiert. Das Security Management hat aber darüber hinaus Aufgaben, die weit in alle Bereiche der Informationsverarbeitung hineinreichen.

Die operative Ebene besteht aus den Prozessen des Service Support, welches die Prozesse beinhaltet, die für die mittelbare oder unmittelbare Umsetzung verantwortlich sind. So findet hier die gesamte Kommunikation mit den Anwendern statt sowie die Verwaltung aller Änderungen. Im Service Support sind alle Prozesse eng mit den Zielen der Informationssicherheit verbunden.

3.4 Security Management auf der taktischen Ebene

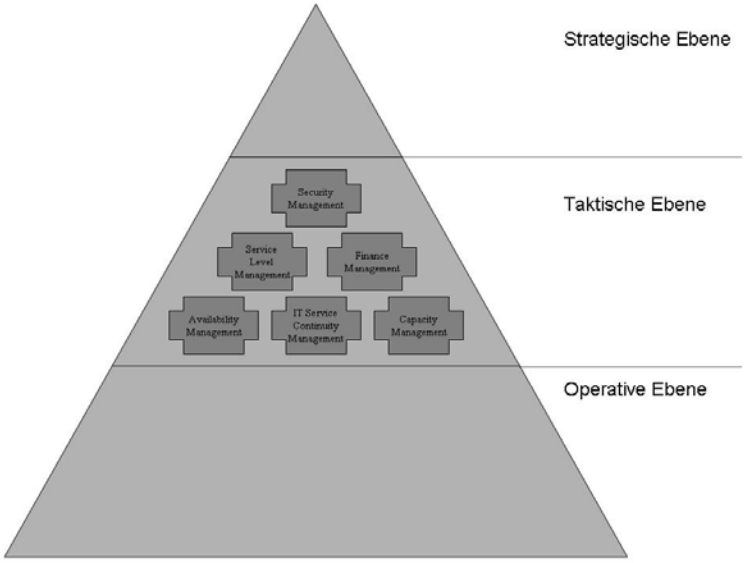


Abbildung 8: Security Management auf der taktischen Ebene

Die taktische Ebene bei ITIL wird durch das Service Delivery beschrieben. Hier sind die Verfahren und Prozesse definiert, die für die Planung und das Controlling von IT-Services nötig sind.

- Service Level Management
- Availability Management
- Capacity Management
- Finance Management für IT Services
- IT Service Continuity Management

Der Security Management Prozess ist ebenfalls ein taktischer Prozess.

Im folgenden Kapitel werden die Schnittstellen zwischen den Prozesse des Service Delivery und dem Security Management beschrieben.

3.4.1 Service Level Management

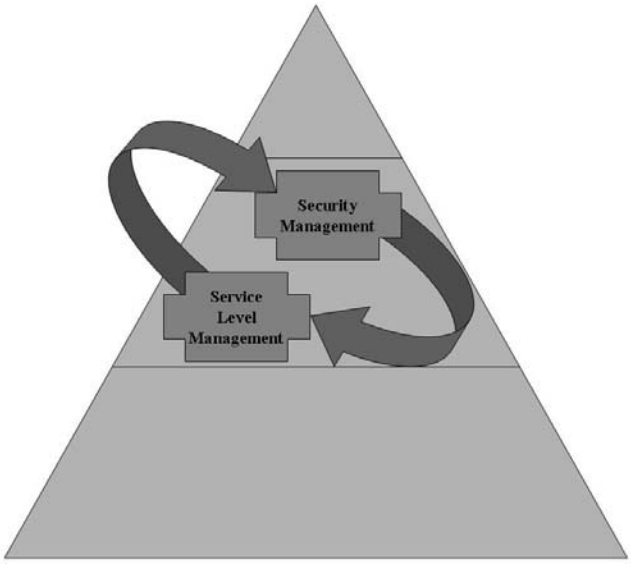


Abbildung 9: Security & Service Level Management

Das Service Level Management bildet die Schnittstelle zum Kunden, um dessen Anforderungen mit dem Leistungsangebot des IT-Dienstleisters abzugleichen.

Ziel ist es, eine beiderseits verbindliche Vereinbarung über Umfang und Qualität der zu erbringenden IT-Dienstleistungen (IT-Services) zu erzielen.

Solch eine Vereinbarung wird Service Level Agreement (SLA) genannt und beschreibt vollständig, welche IT-Services zu erbringen sind. Ist ein IT-Service in diesem SLA nicht beschrieben, darf er nicht erbracht werden, bis er in dem SLA aufgenommen worden ist.

Der Grund hierfür liegt darin, dass seitens ITIL durch das Service Level Management Nebenabreden ausgeschlossen werden sollen, da diese zwangsläufig zu Unklarheiten darüber führen würden, welche IT-Services aktuell erbracht werden dürfen und welche nicht. Es wäre dann unklar, ob ein IT-Service nur deshalb nicht in dem SLA dokumentiert ist, weil dieser dem Kunden zu teuer gewesen wäre, oder weil er aus anderen Gründen, beispielsweise der Informationssicherheit, nicht enthalten ist.

Dieses stellt die Hauptaufgabe des Service Level Managements sehr anschaulich dar, nämlich die Bemühung, alle Anforderung des Kunden, die aus dessen Geschäftsprozessen resultieren, zu erkennen und in IT-Services umzusetzen. Dazu zählen auch die Anforderungen, die dem Kunden nicht bekannt sind oder wichtig erscheinen, wie zum Beispiel Datenschutz, gesetzliche Bestimmungen oder Verfügbarkeitsanforderungen.

Das bedeutet nicht, dass ein IT-Dienstleister dem Kunden vorschreiben kann, welche IT-Services dieser tatsächlich braucht, sondern hier ist der IT-Dienstleister aufgefordert, den Kunden auf mögliche fehlende Anforderungen aufmerksam zu machen und ihn in Bezug darauf zu beraten, welches Maß an Risiko damit verbunden ist. Die Frage, ein wie hohes Risiko der Kunde tatsächlich bereit ist zu akzeptieren, muss dieser dann selbst beantworten.

Der Service Level Management Prozess ist also verantwortlich für den Inhalt der SLA, sorgt aber auch dafür, dass die tatsächliche Erbringung der IT-Services gemessen werden kann und liefert dem Kunden die Berichte darüber in einem definierten Format zu.

Basis für das SLA bildet auf Seiten des IT-Dienstleisters der Service-Katalog, der alle IT-Services enthält und detailliert beschreibt.

Weitere wichtige Begriffe im Service Level Management sind Operational Level Agreements (OLA), die eine Service-Vereinbarung mit den internen Leistungserbringern, beispielsweise dem Service Desk, sowie Underpinning Contracts (UC), welche die Einbindung von externen Partnern regelt wie beispielsweise Hardwarelieferanten oder externen Systemexperten.

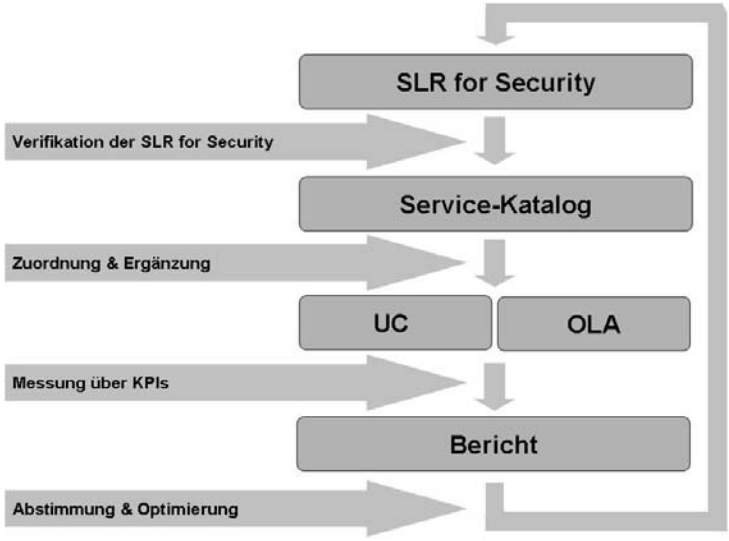


Abbildung 10: Security Aufgaben Service Level Management

Bezogen auf die Informationssicherheit sind die Aufgaben des Service Level Management folgende:

- Aufnahme aller Anforderungen des Kunden an die Informationssicherheit, den Service Level Requirements (SLR) for Security. Die Erfahrung aus vielen Projekten zeigt, dass der geeignete Weg, diese zu erlangen eine Untersuchung der Geschäftsprozesse ist, bei denen die spezifischen SLR for Security herausgearbeitet werden. Das Ergebnis muss die Anforderungen umfassen, die der Kunde an die Erbringung seiner Geschäftsprozesse stellt.
- Eine genaue Prüfung, ob eine Anforderung durch den IT-Dienstleister erbracht werden kann ist notwendig, da dieser sonst die Verantwortung für Maßnahmen übernimmt, die nicht in seinem Verantwortungsbereich liegen oder nicht durch ihn erbracht werden können.

- Ein Abgleich mit dem Service-Katalog des IT-Dienstleisters, hier speziell mit den Security Baselines, stellt fest, wie die Anforderungen durch bestimmte Maßnahmen erfüllt werden können. Hier wird beispielsweise häufig viel Zeit mit Diskussionen darüber verbracht, welches Anti-MalWare Programm besser ist. Da die IT-Dienstleister ihre festen Lieferanten haben, sollten hier die Maßnahmen und die Berichte so definiert werden, dass mögliche Bedenken eines Kunden auf Basis von nachweisbaren Fakten ausgeräumt werden können. Andererseits ist es hier wichtig, gerade diese Punkte durch das Service Level Management genau im Auge zu behalten, da kleine Abweichungen hier schnell zu einer größeren Verstimmung führen können. Ebenfalls sollte ein IT-Dienstleister der Anregung und der Kritik eines Kunden gegenüber aufgeschlossen sein und nicht dogmatisch nur an seiner Vorstellung festhalten, wie man Informationssicherheit erreichen kann.
- Anforderungen, die durch die Security Baselines nicht erfüllt werden können, müssen mit erweiterten Maßnahmen beantwortet werden. Diese werden ebenfalls in dem SLA beschrieben. Dieses führt in der Regel schnell zu höheren Kosten, so dass dann erneut analysiert werden muss, ob der Nutzen durch höhere Sicherheitsziele mit den erhöhten Kosten im Einklang steht. Gerade bei Outsourcing Projekten muss ein Kunde an dieser Stelle im Vorfeld genau seine SLR for Security definieren, um zu einer guten Vergleichbarkeit von Angeboten zu kommen, da beispielsweise jeder Prozentpunkt mehr an Verfügbarkeit etliche Prozentpunkte mehr an Kosten mit sich bringt.
- Der IT-Dienstleister benötigt zur Erbringung der IT-Services meist Dienstleistungen von Dritten, beispielsweise einem Telekommunikationsunternehmen für die Internetverbindung oder einem Softwarehersteller für die Anpassung der Software-Anwendung. Diese Leistungen liegen nicht in dem Verantwortungsbereich des IT-Dienstleisters, daher muss ein UC zwischen dem IT-Dienstleister und dem Dritten geschlossen werden. Die Vereinbarung des UC sollte nicht nur mit dem Kunden abgesprochen werden vielmehr sollte dieser sogar aktiv in die Verhandlungen mit einbezogen werden. Das hat den Vorteil, dass er sich im Falle einer Störung, die durch den Dritten verantwortet wird, bewusst ist, dass der IT-Dienstleister seine SLAs eingehalten hat.

- Um die Sicherheitsziele, die im SLA vereinbart worden sind, in die operativen IT-Prozesse einzuführen, werden OLAs mit den beteiligten Prozessverantwortlichen abgeschlossen. Hier wird pro Sicherheitsziel aus dem SLA eine genauere Anweisung gegeben, welche Aufgaben damit verbunden sind. Zum Beispiel kann in einem SLA die „sichere Entsorgung von alten Datenträgern“ vereinbart sein. In einem OLA wird definiert, welche Auswirkungen auf die Entsorgung von Disketten, Tapes, USB-Sticks, Festplatten in Arbeitsplatz-PCs und Servern, Ausdrucke von Protokolldateien und weiteren Datenträgern damit verbunden sind. Ebenso müssen die UC definiert werden, in denen festgelegt wird, wann welche Dienstleistung von einem Dritten erbracht werden muss, damit der IT-Dienstleister die Sicherheitsziele einhalten kann.
- Um die Zielerreichung der einzelnen Sicherheitsziele messen und bewerten zu können, muss ein Berichtswesen auf vergleichbaren Metriken aufgesetzt werden. Bei ITIL definiert man dazu Kennzahlen, die so genannten Key Performance Indicators (KPI) und die Performance Kriterien. Während die KPIs die messbaren Kennzahlen darstellen, handelt es sich bei den Performance Kriterien um das zu erreichenden Niveau. Diese KPIs sollten von Kunden und IT-Dienstleistern gemeinsam ausgewählt werden, da sie einerseits in vielen Fällen zur Abrechnung der Services dienen, und daher belastbar und von beiden Seiten akzeptiert sein sollten, speziell wenn einer Malus-Regelung, also der Preisminderung bei schlechter Service-Qualität, auch eine Bonus-Regelung gegenübersteht, also einer Preiserhöhung bei besserer Qualität. Andererseits kann der Kunde diese KPIs nutzen, um seine eigene Produktivität zu verbessern, beispielsweise um Schulungsbedarf bei bestimmten Software-Anwendungen zu identifizieren.
- Auf Basis der KPIs sollten regelmäßige Berichte an den und Treffen mit dem Kunden stattfinden, um Optimierungspotential zu identifizieren und auf mögliche – positive wie negative – Trends aufmerksam zu machen und eine Lösung dafür zu finden. In diesen regelmäßigen Treffen sollten ebenfalls die Gültigkeit der definierten Ziele der Informationssicherheit geprüft und neue Projekte des Kunden in Bezug auf die IS untersucht werden.

3.4.2 Service Level Agreement

Ein Service Level Agreement ist kein Prozess im Sinne von ITIL, jedoch ein wichtiges Element des Security Managements. Daher wird es hier als separates Kapitel aufgeführt, obwohl es ein Ergebnistyp des Service Level Managements ist.

Die Ziele innerhalb der SLA werden in einem Absatz über die Sicherheitsziele, der so genannten Security Section beschrieben und dienen als Anforderungen für den Security Management Prozess.

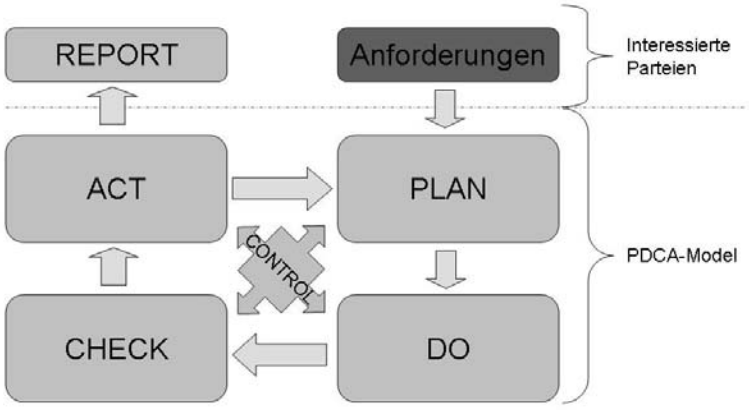


Abbildung 11: Anforderungen an das Security Management

Es ist wichtig, dass die Ziele in messbaren Größen definiert werden, damit ein gemeinsames Verständnis erreicht wird.

Die Security Section enthält allgemeine und spezielle Bereiche, in denen die Maßnahmen und KPIs beschrieben sind.

Die Ziele hängen je nach Unternehmen stark davon ab, ob bereits ein durchgängiges ISMS implementiert ist oder ob ein solches erst aufgebaut werden soll. Folgende Fragestellungen müssen beantwortet werden:

- Was sind die SLR for Security des Kunden?
- Welche Maßnahmen aus dem Service-Katalog eignen sich, um diese SLR for Security zu erreichen?
- Welche zusätzlichen Maßnahmen müssen getroffen werden, um diese SLR for Security zu erreichen?
- Welche UC werden benötigt, um die SLR for Security einzuhalten?
- Welches sind die Pflichten, die der Kunde erfüllen muss?

Beispielhaft sei hier wiederum die „sichere Entsorgung von alten Datenträgern“ genannt. Nehmen wir einmal an, es handelt sich um eine Behörde aus Schleswig-Holstein, die eine Entsorgung der Datenträger bei einem Dienstleister vornehmen muss, der ein Datenschutz Gütesiegel des Landes Schleswig-Holstein besitzt. Damit würden die Fragen wie folgt beantwortet werden:

- Was sind die SLR for Security des Kunden?
  - Entsorgung von elektronischen Datenträgern und Papier durch einen zertifizierten Dienstleister gemäß Datenschutz Gütesiegel.
- Welche Maßnahmen aus dem Service-Katalog eignen sich, um diese SLR for Security zu erreichen?
  - Zentrale Sammlung von mobilen Datenträgern
  - Identifikation von Datenträgern (Tapes) zur Entsorgung (CMDB)
  - Registrierung von Datenträgern (Tapes) zur Entsorgung (CMDB)
  - Bericht der Entsorgung an Kunden.

- Welche zusätzlichen Maßnahmen müssen getroffen werden, um diese SLR for Security zu erreichen?
  - Entsorgung durch externen Dienstleister gemäß Datenschutz Gütesiegel
- Welche UC werden benötigt, um die SLR for Security einzuhalten?
  - Vereinbarung mit externem Dienstleister über Art der Entsorgung und Verfügbarkeit der Dienstleistung.
- Welches sind die Pflichten, die der Kunde erfüllen muss?
  - Bei mobilen Speichern der Anwender: Lieferung der mobilen Speicher an zentrale Sammelstelle (Datenträgertonne)
  - Bei Papier: Lieferung des Papiers an zentrale Sammelstelle (verschlossene Papiertonne).
- In die OLAs, die das Service Level Management ebenfalls steuert, werden dann die Bereiche des Service-Katalogs aufgenommen und in Verfahrensbeschreibungen konkretisiert.
- Als Beispiel sei hier die „Registrierung von Datenträgern zur Entsorgung (CMDB)“ genommen. Eine OLA würde folgende Schritte beschreiben:
- Datenträger in der CMDB identifizieren
- Datenträger auf „zur Entsorgung“ markieren
- Ersatzbeschaffung veranlassen
- Datenträger zur Entsorgung vorbereiten.

Normalerweise sind einfache Verfahren mit wenigen Stichpunkten beschrieben. Komplexere Verfahren und solche, die selten durchgeführt werden, sind detaillierter dokumentiert.

3.4.3 Availability Management

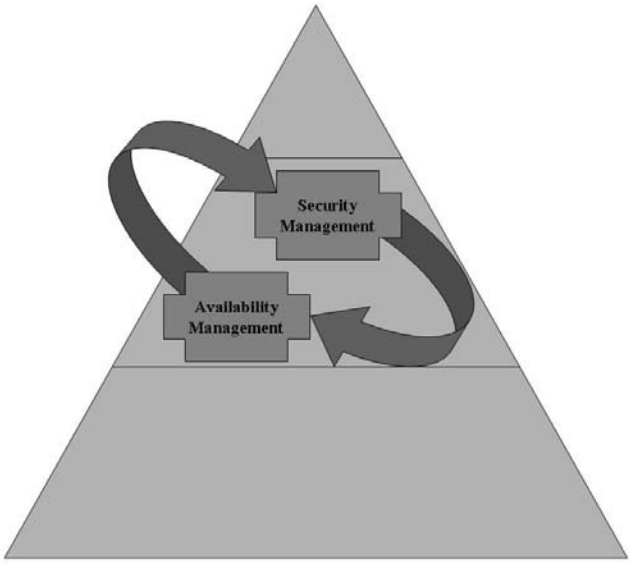


Abbildung 12: Security & Availability Management

Bis vor kurzem war das Security Management Bestandteil des Availability Managements, da eine der Säulen der Informationssicherheit die Verfügbarkeit ist.

Wie dieses Buch zeigt, umfasst IS aber sehr viel mehr als nur die Verfügbarkeit von Systemen, nämlich ebenso die Attribute Vertraulichkeit und Integrität. Sicherheit ist somit die Summe aus allen drei Säulen. Das bedeutet in der Folge, dass jede der drei Säulen einen gewissen Grundschutz enthalten muss, um eines der anderen Ziele zu erreichen. Da die sehr fokussierte Sicht auf Verfügbarkeit nicht mehr ausreichte, wurden Availability Management und Security Management in zwei Prozesse aufgeteilt.

Bei dem Availability Management verbleiben die Aufgaben, folgende Qualitätsmerkmale sicherzustellen:

- Die Zuverlässigkeit (engl. Reliability) beschreibt einen zeitlichen Qualitätsaspekt, nämlich dass ein System oder ein Service in der benötigten und vereinbarten Zeit mit den definierten Funktionen zu einem festgelegten Maß an Qualität zur Verfügung steht. Als Beispiel sei ein Buchhaltungssystem genannt, das in den Kernarbeitszeiten (Montag bis Freitag von 8:00 – 16:00 Uhr) den Anwendern mit einer definierten maximalen Antwortzeit zur Verfügung steht.
- Die Wartbarkeit (engl. Maintainability) gibt an, mit welchem Aufwand ein System gewartet werden kann und welche Auswirkungen diese Wartung auf andere Systeme und IT-Services hat. Eine Wartung ist beispielsweise eine Erweiterung, Erneuerung oder Reparatur von Hardwarekomponenten, aber auch ein Update, Upgrade oder Patch bei Software-Anwendungen und Firmware. Die Wartbarkeit hängt stark davon ab, wie gut die Systeme dokumentiert sind, ob ein systematischer und nachvollziehbarer Aufbau des Datenmodells erfolgt ist und ob bei der Erstellung eines Systems bereits an zukünftige Anforderungen und Funktionalitäten gedacht worden ist. Häufig werden Ideen für neue Systeme und Software-Anwendungen erst einmal prototypisch umgesetzt. Bei einem Prototypen wird erfahrungsgemäß nicht in besonderem Maße auf Wartbarkeit geachtet, da dieser schnell gegen ein neues System ersetzt werden soll. Typisch für Prototypen sind festkodierte Adressen, schlechte Erweiterbarkeit aufgrund fehlender Schnittstellen und die Missachtung festgelegter Programmierrichtlinien. Erfahrungsgemäß halten solche Provisorien länger, als es ursprünglich geplant war und reduzieren dadurch die Wartbarkeit der gesamten restlichen IT-Infrastruktur. Besonders bei Wartungsmaßnahmen, die aufgrund von Security Incidents durchgeführt werden müssen, ist es besonders wichtig, dass eine schnelle und problemlose Wartung möglich ist, da sonst die Sicherheitslücke unverhältnismäßig lange besteht und andere Systeme und IT-Services in Mitleidenschaft gezogen werden können, beispielsweise durch längere Abschaltzeiten vom Internet bei einer akuten MalWare-Epidemie.
- Servicefähigkeit (engl. Serviceability) beschreibt, wie die Unterstützung durch Dritte in Bezug auf die Verfügbarkeit,

Wartbarkeit und Zuverlässigkeit der Komponenten gewährleistet ist, die unter der Verantwortung dieser Dritten stehen. Es handelt sich nicht um eine konkrete Messgröße, sondern um die Verfügbarkeit, die durch externe Dienstleister sichergestellt werden muss.

- Die Ausfallsicherheit (engl.: Resilience) wird auch Robustheit genannt und ist beispielsweise im Flugzeugbau schon seit Jahrzehnten eine der Hauptpflichten für Systeme, die für den Flugbetrieb zuständig sind. Solche Konzepte, auch Graceful Degradation (schrittweise Abschaltungen) genannt, führen dazu, dass nicht ein gesamtes System oder ein Service ausfällt, wenn eine Komponente den Dienst verweigert, sondern sich nur diese eine Komponente abschaltet und die verbleibenden Systeme nicht daran hindert, weiterhin ihre Arbeit zu verreichten. In der IT spricht man heute von so genannten Bottle Necks (Flaschenhälsen) oder auch Single Points of Failures, wenn durch eine Störung gesamte Services oder sogar die gesamte IT-Infrastruktur zum Erliegen gebracht werden.

Die Hauptaufgabe des Availability Managements in Bezug auf das Security Management sind die Planung und Umsetzung der Ziele der Informationssicherheit unter dem Aspekt der Verfügbarkeit. Dieses wird durch die Auswahl geeigneter KPIs für Messungen und Berichte erreicht sowie durch die Auswahl der Maßnahmen zur Sicherung der Sicherheitsziele.

Darüber hinaus hat das Availability Management die Aufgabe, die Komplexität der IT Infrastruktur zu überwachen mit dem Ziel, kritische Flaschenhälse zu identifizieren und zukünftig zu vermeiden.

Aus diesem Grund unterstützt das Availability Management das Security Management bei Änderungen an der IT-Infrastruktur mit Analysen und Maßnahmenplanungen.

Ebenfalls wichtig ist die dauerhafte Überwachung (Monitoring) der bestehenden IT Infrastruktur. Abweichungen vom Verfügbarkeitsplan werden an das Security Management gemeldet, da die Ursache hierfür ein Security Incident sein kann. Ebenso werden Trend und regelmäßige Berichte erstellt, die das Security Management auswertet.

3.4.4 Capacity Management

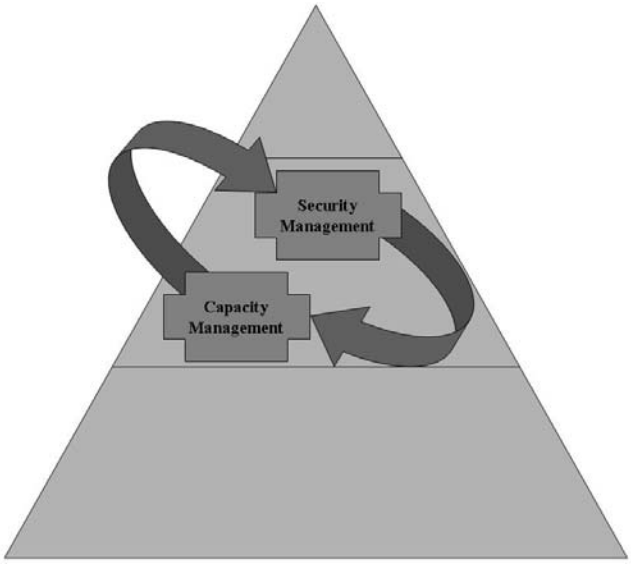


Abbildung 13: Security & Capacity Management

Das Capacity Management wird manchmal auch Performance and Capacity Management genannt, was der Tatsache Rechnung trägt, dass die Leistungsfähigkeit (Performance) eines IT-Service direkt mit dessen Kapazitäten (Capacity) in Verbindung steht.

Die Aufgabe des Capacity Managements ist die Sicherstellung, dass alle eingesetzten Ressourcen und IT-Services wirtschaftlich eingesetzt werden. Ein wesentlicher Aspekt liegt in der Planung, da geplante Entscheidungen in jedem Fall wirtschaftlicher sind als ungeplante.

Das Capacity Management ist in drei Bereiche aufgeteilt:

Im Business Capacity Management werden mittel- und langfristige Planungen vorgenommen. Um hier eine ausgewogene Basis zu erhalten, wird die Planung des Unternehmens genutzt, um die nötigen IT-Services gezielt darauf abzustimmen. Dieses mittel- und langfristige Aufnehmen und Bewerten von Anforderungen wird ***Demand Management*** genannt.

Wichtige Indikatoren für die mittel- und langfristige Unternehmensentwicklung sind

- Strategieplanung,
- Personalentwicklungspläne,
- Bereichsziele,
- Branchenvergleich,
- mittel- und langfristige Releaseplanung und
- Techniktrends.

Für das Security Management sind die Bedrohungstrends zusätzlich wichtig, die Rückschlüsse auf zukünftige Bedrohungen für das Unternehmen zulassen, abhängig von Branche und Grad der Technologienutzung.

Das Business Capacity Management extrapoliert aus diesen Unterlagen die relevanten Zusammenhänge für die IT-Services und übersetzt dieses in Ziele für die IT-Infrastruktur. Folgende Ergebnistypen sollten dann für die mittel- und langfristige Planung der IT-Services zur Verfügung stehen:

- IT-Roadmap, in der alle IT-Services im Überblick beschrieben sind und die einen sinnvoll planbaren Zeitraum abdeckt. Üblicherweise werden hier drei bis fünf Jahre als Planungshorizont genommen. Je weiter eine Planung in die Zukunft geht, desto gröber wird diese.
- Risikotrends, beschreiben die aus den Bedrohungstrends abgeleitete Entwicklung von Risken, die mit den alten und neuen Technologien basierend auf der IT-Roadmap einhergeht. Diese Risikotrends werden durch das Security Management erstellt.

- Empfehlungen, wie die Planung der IT-Services die Unternehmensplanung optimal unterstützen kann. Dem Security Management kommt hier besonders die Rolle zu, frühzeitig Chancen und Risiken zu erkennen und im Sinne der Unternehmensziele abwägen zu können. Dieses zeigt anschaulich, dass das Security Management nicht nur eine technische Aufgabe ist, die umgesetzt werden muss, sondern hier sind Führungsqualitäten gefragt, da gerade in der frühen Planungsphase, in der die Budgets aufgeteilt werden, ein hohes Maß an Standfestigkeit gefordert ist.

Das Service Capacity Management stellt die tatsächliche Erbringung der vereinbarten IT-Services sicher, indem diese permanent überwacht und analysiert werden. Das Service Capacity Management ist zudem für die Planung der kurzfristig anstehenden Serviceänderungen oder –einführungen zuständig.

Zur Überwachung werden definierte KPIs ermittelt und mit den tatsächlich vereinbarten verglichen. Das Service Capacity Management betrachtet keine einzelnen Ressourcen innerhalb eines IT-Services wie beispielsweise Systeme oder Software-Anwendungen, sondern den IT-Service, der beim Anwender ankommt. Da durch die KPIs viele Komponenten indirekt mit überwacht werden, eignen sich die KPIs des Service Capacity Management als ein guter Indikator dafür, ob Störungen der Leistungserbringung aufgetreten oder ob diese zu erwarten sind. Diese KPIs sind daher wertvolle Hinweise für das Security Management, der diese mit anderen KPIs in einen Zusammenhang bringen kann, um Security Incidents abzuleiten.

Das Ressource Capacity Management plant und überwacht die einzelnen Komponenten der IT Infrastruktur. Hier wird gemäß der Komplexität der IT-Infrastruktur eine Vielzahl an Messpunkten angesprochen, die schnell dazu führen kann, den Überblick und damit den Sinn für das Wesentliche zu verlieren. Hier ist es besonders wichtig, die richtigen Messpunkte zu identifizieren, die sich entweder an zentralen Stellen der IT-Infrastruktur befinden oder besonders kritisch für diese sind. Beispiele für häufig gewählte Messpunkte sind das Netzwerk, da hier die meisten Angriffe geschehen, oder die Speicherauslastung, da ein schneller Anstieg die Speicherbedarfs auch auf eine unerlaubte Nut-

zung hinweisen kann, beispielsweise auf die Speicherung von Filmen oder MP3-Dateien.

Eine der Hauptaufgaben beim Ressource Capacity Management ist zudem die Auswahl der Protokolldatei-Parameter, die für Analysen zur Verfügung stehen, sei es zur Aufklärung eines Security Incidents oder zu anderen Analysezwecken.

Das Security Management muss bestimmen, wohin die Protokolldateien zu speichern sind, wer auf diese zugreifen darf und wie diese gegen Veränderungen zu schützen sind.

3.4.5 IT Service Continuity Management

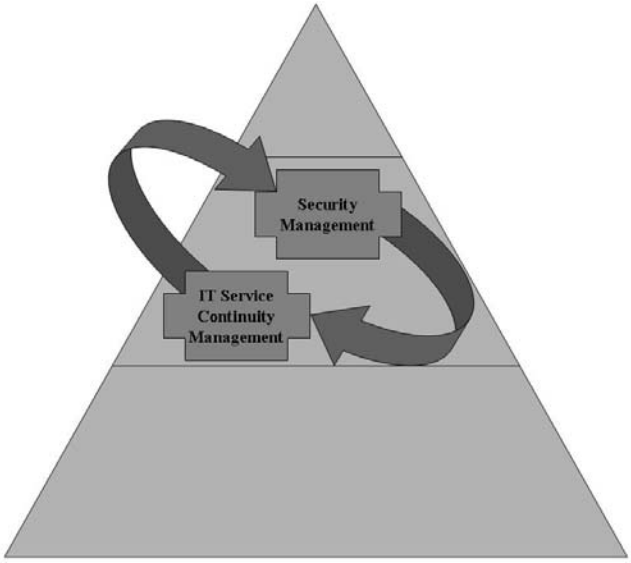


Abbildung 14: Security & Continuity Management

Das IT Service Continuity Management ist verantwortlich für die Frage, ob die IT-Services nach einem Notfall in einer definierten Zeit wieder zur Verfügung stehen.

Gründe für Notfälle sind vielfältig und teilweise trivial. So kann ein Kurzschluss in der Klimaanlage verheerende Folgen haben. Die häufigsten Gründe für Notfälle sind Feuer und technische Ausfälle. Regional können auch Erdbeben, Hochwasser und Schneekatastrophen zu Notfällen führen. Eine große Bedrohung stellen heute zudem Sabotage und Terrorismus dar.

Notfälle betreffen normalerweise nicht nur IT-Services, sondern auch Anwender, Logistik und Geschäftsprozesse. Die Sicherstellung dieser Bereiche während eines Notfalls ist Aufgabe des Business Continuity Managements, das einen separaten, beziehungsweise übergeordneten Prozess darstellt.

Da Notfälle die Verfügbarkeit der IT-Services betreffen, handelt es sich um eine erweiterte Aufgabe des Security Managements. Da aber speziell beim IT Service Continuity Management ein hoher Verwaltungsaufwand anfällt, ist es sinnvoll, diesen Prozess separat zu behandeln.

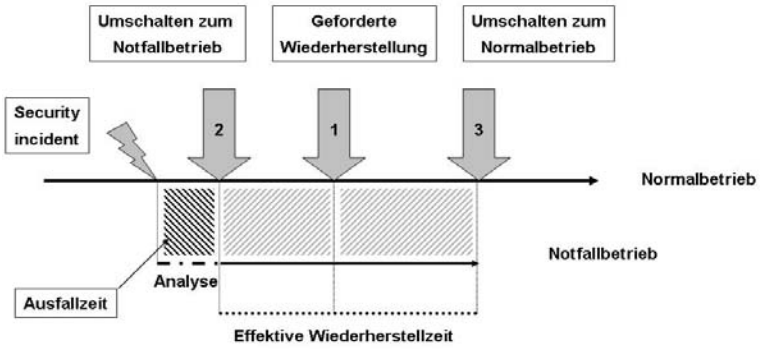


Abbildung 15: Vom Normalbetrieb zum Notfallbetrieb

Der Zusammenhang zwischen einem Incident und einem Notfall wird durch Abbildung 15 beispielhaft beschrieben.

Nach einem Ausfall eines IT Services, der durch einen Incident ausgelöst worden ist, muss analysiert werden, ob dieser IT-Service durch Maßnahmen des normalen IT-Betriebes zur geforderten Zeit (1) wiederhergestellt werden kann. Wenn dieses nicht erreicht werden kann, muss auf einen Notfallbetrieb umgeschaltet werden.

Ein Notfall ist eine Incident, der einen IT-Service so stark beeinträchtigt, dass dieser nicht während der geforderten Zeit wiederhergestellt werden kann.

Die Aufgaben des IT Service Continuity Managements sind folgende:

- Analyse der Auswirkung, welche die Unterbrechung eines IT-Services auf die Ziele hat, die in einem SLA definiert worden sind
- Identifikation geschäftskritischer IT-Services
- Definition der Mindestwiederherstellzeit
- Definition und Sicherstellung von Maßnahmen, um Notfälle zu erkennen, diesen vorzubeugen, die Auswirkung zu vermindern oder das Eintrittsrisiko herabzusetzen
- Verfahren implementieren, die einen Wiederanlauf nach einem Notfall ermöglichen
- Erstellung, Test und Pflege eines Notfallplans

Die Aktivitäten des IT Service Continuity Managements sind in fünf Phasen eingeteilt:

1. Initiierung
2. Anforderung
3. Strategie
4. Implementierung
5. Operatives Management

In der Initiierungsphase wird die IT Service Continuity Policy (ITSC-Policy) erstellt, die einerseits die Regeln und Grundsätze festlegt, die für die Notfallplanung gelten, andererseits die Unterstützung durch die Unternehmensleitung ausdrücken.

Die Anforderungsphase beinhaltet die Aktivitäten der Schadensauswirkungsanalyse, der Risikoanalyse und der Auswahl der geeigneten Strategie.

- Durch eine Schadensauswirkungsanalyse wird festgestellt, wie lange ein IT-Service maximal ausfallen kann, ohne dass die Geschäftsprozesse davon ernsthaft gefährdet sind.

- In einer Risikoanalyse werden Betriebsmittel (Assets) dahingehend untersucht, ob für diese Bedrohungen existieren und ob Schwachstellen diese Bedrohung fördern.

In der Strategiephase werden auf Basis der Analyseergebnisse die Ziele für IT Service Continuity in dem SLA definiert.

- Die Auswahl der geeigneten Strategie passiert auf Basis des Maßnahmenkataloges des IT-Dienstleister. Hierdurch wird festgelegt, wie die Ziele im SLA erfüllt werden können.
- Um kritische Geschäftsprozesse sicherzustellen müssen eventuell Maßnahmen gewählt werden, die nicht standardmäßig im Maßnahmenkatalog enthalten sind. Hier müssen dann zusätzliche Maßnahmen entwickelt und im SLA vereinbart werden.
- Es gibt sechs Strategien, wie gegen Notfälle eines IT-Services vorgesorgt werden kann. Normalerweise werden Mischformen aus diesen sechs Strategien gewählt, um zu einer optimalen Lösung zu kommen:

1. Die mutigste Strategie ist es, keinerlei Planung für den Notfall zu treffen. Dieses ist weit verbreitet, jedoch können es sich die wenigsten Unternehmen leisten, keine Vorsorge zu treffen. Der Gesetzgeber hat hier bereits erste Bemühungen unternommen, solch eine übertriebene Risikobereitschaft einzudämmen, nämlich durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).

2. Manchmal sind noch alte Verfahren verfügbar, beispielsweise auf netzwerkunabhängigen Arbeitsplatz-PCs oder als Papierformulare, die mittlerweile durch IT-Services abgelöst worden sind. Solche alten Verfahren können als zeitlich begrenzte Lösungen dann genutzt werden, wenn die Verfahren (a) noch dem Geschäftsprozess entsprechen, und beispielsweise die Formulare an Neuerungen jeweils angepasst worden sind. Außerdem müssen noch (b) Anwender in der Lage sein, diese alten Verfahren anzuwenden. Abschließend muss (c) sichergestellt sein, dass alle Arbeitsergebnisse solcher alten Verfahren in dem IT-Service nachgepflegt werden können, nachdem dieser wiederhergestellt worden ist.
3. Hohe Kosten bei einem professionellen Ausweichrechenzentrum führen dazu, dass Unternehmen sich mit anderen Unternehmen darauf verständigen, diesen während eines Notfalls zu helfen und beispielsweise Rechenzentrumsfläche oder sogar Systeme zur Verfügung zu stellen. Diese beiderseitigen Abmachungen müssen jedoch dahingehend genau untersucht werden, ob die technischen Voraussetzungen passen und alle Änderungen im anderen Unternehmen jeweils dahingehend untersucht werden, ob danach noch die Fähigkeit vorhanden ist, „IT-Service Asyl“ zu gewährleisten oder zu nehmen. Die meisten solcher Abmachungen scheitern an organisatorischen oder technischen Gründen, einige bereits während der Verhandlung. Fragen des Zutritts durch Mitarbeiter des fremden Unternehmens oder Nutzung von Räumlichkeiten können nicht einvernehmlich gelöst werden.
4. Die folgenden drei Strategien sind abhängig von der Maximalen Wiederanlaufzeit (MWZ) der IT Services. Bei längerer MWZ kann ein Cold Standby gewählt werden, also bereits vorbereitete Serverschränke oder Rechenzentrumsfläche, die infrastrukturell einfach angebunden werden kann. Solche vorbereiteten Flächen können auch mobile Rechenzentrumscontainer sein, die an einem definierten Andockpunkt angeliefert werden. Hier muss durch Auswahl eines oder besser mehrerer Andockpunkte sichergestellt werden, so dass diese nicht selbst durch den Notfall betroffen sind. Die Systeme müssen entweder beschafft werden, beispielsweise über Liefervereinbarungen mit Hardwareherstellern, oder können für die Zeit des Notfalls umgewidmet werden. Hier werden häufig Test- und

Konsolidierungssysteme gewählt, da diese sehr produktionsnah sind. Durch die Auswahl des geeigneten Datensicherungsverfahrens (Backup) muss sichergestellt werden, dass die Daten für den IT-Service in der Aktualität vorliegen, die in den SLA gefordert wird. Dieses wird durch regelmäßige Auslagerung oder Onlinebackup bei einem Dienstleister erreicht.

5. Die nächste Stufe stellt das Warm Standby dar, durch Nutzung eines bereits ausgestatteten Rechenzentrums oder Serverraums. Hier sind die Systeme bereits vorhanden, die Daten müssen lediglich noch eingespielt werden, und die Applikationen müssen aktualisiert und einmal auf richtige Funktionalität durchgetestet werden. Ein Warm Standby ist sowohl in eigenen Räumen wie auch bei einem professionellen Ausweichrechenzentrum möglich. Erfahrungen aus zahlreichen Projekten haben gezeigt, dass professionelle Hilfe hier viele Stunden Wiederanlauf spart und zahlreiche Stolpersteine vermeidet, die bei einer Umschaltung während eines Notfalls immer wieder auftreten.
6. Die höchste Stufe ist das Hot Standby, also das permanente Mitlaufen der Systeme parallel zum Produktionsbetrieb. Heute nutzt man IT-Services, die hohe Anforderungen an die MWZ haben, in mehreren Standorten produktiv, so dass ein einfaches Abschalten der betroffenen Lokalität ohne Betriebsunterbrechung möglich ist.

In der Implementierungsphase wird die Strategie in Verfahren und Pläne umgesetzt. Diese Phase umfasst folgende Punkte:

- Die Wahl der Organisation für das IT Service Continuity Management sowie die Bestimmung des Krisenstabes. Hierbei muss festgelegt werden, wer Krisenmanager ist, und welche Kompetenzen dieser hat. Darüber hinaus sind die weiteren Mitglieder des Krisenstabes zu definieren und deren Aufgaben zu beschreiben. Mitglieder eines Krisenstabes sollten aus folgenden Abteilungen kommen:
  - Geschäftsführung
  - Security Manager
  - Öffentlichkeitsarbeit
  - Leistung Informationstechnologie
  - Personal
  - Haus- und Gebäudetechnik (meist auch für physische Sicherheit zuständig)
  - Weitere Mitglieder sollten je nach Kritikalität dazu genommen werden, beispielsweise Fachbereiche mit hohen Risiken.
- Für die Planung der Implementierung müssen die Dokumente und Verfahren festgelegt werden, die durch das IT Service Continuity Management verantwortet und gepflegt werden. Hierbei ist darauf zu achten, dass je nach gewählter Strategie und Kritikalität jedes Unternehmen einen sehr unterschiedlichen Detaillierungsgrad haben wird. Reine Copy-and-Paste Verfahren, also das direkte Übernehmen einer erfolgreichen Planung anderer Unternehmen sollte vermieden werden. Die notwendigen Dokumente sind:
  - Notfallplan
  - Wiederherstellungspläne
  - Plan für Öffentlichkeitsarbeit

- Handakten-Planung; hierbei muss berücksichtigt werden, welche Unterlagen, beispielsweise Handakten, lokal gespeicherte Dokumente, E-Mail-Verzeichnisse und Unterlagen auf USB-Sticks während eines Notfalls genutzt werden müssen.
- Eine Battle-Box beinhaltet die Unterlagen, die von dem Krisenstab oder den Wiederherstellungs-Teams zuerst benötigt werden. In einer Battle-Box sind üblicherweise

  - Aktuelle Telefonliste mit privater Erreichbarkeit
  - Schadensbeurteilungsvordrucke
  - Adresse der Krisenzentren
  - Lagepläne
  - Durch die Nutzung moderner Technik, zum Beispiel Smartphones, können diese Battle-Boxes digital in der jeweils aktuellen Version bei jedem Mitglied des Krisenstabes verfügbar sein.

- Die Maßnahmenplanung unterscheidet zwischen präventiven und reaktiven Maßnahmen. Während durch die präventiven Maßnahmen die Auswirkungen durch einen Notfall gemindert werden sollen, werden reaktive Maßnahmen geplant, um die Zeit des Ausfalles zu minimieren. Die reaktiven Maßnahmen sind diejenigen, die aufgrund der gewählten Strategie vorgenommen werden. Lediglich das Hot Standby kann bis zu einer präventiven Maßnahme ausgebaut werden.
- Die Wiederherstellungsverfahren sind detaillierte Arbeitsanweisungen für die jeweiligen Wiederherstellungs-Teams, für das Vorgehen, um einen IT-Service in einer definierten Zeit wieder zum Laufen zu bekommen. Bei diesem Verfahren muss auf die Aktualität und den Bezug zum Produktionssystem geachtet werden. Bei einer Änderung an diesem muss sichergestellt werden, dass die Verfahren noch durchführbar sind.
- Am Abschluss der Implementierungsphase steht ein initialer Test, der die oben aufgeführten Schritte in seiner Gesamtheit unter realistischen Bedingungen testen soll, um Stolpersteine oder gravierende Hindernisse frühzeitig zu finden.

Die fünfte Phase beschreibt das operative Management, mit folgenden Aufgaben:

- Schulung und Continuity Marketing sollen dafür sorgen, dass das Thema Notfallplanung und die damit verbundenen Aufgaben unternehmensweit verinnerlicht werden und die Berührungsängste bezüglich des Themas gemindert werden,
- Reviews der Planung und Dokumentation ermitteln Optimierungspotentiale,
- Regelmäßige Notfalltests führen zu einer Geläufigkeit und minimieren das Risiko während eines Notfalls,
- das Change Management muss bei allen Änderungen prüfen, ob die Notfallplanung und die Wiederherstellungsverfahren betroffen sind und
- die Revision überprüft regelmäßig, ob mit der aktuellen Notfallplanung die Anforderungen aus den Geschäftsprozessen erfüllt werden.

Die Aufgaben des Security Managements sind eng mit den beschriebenen Aufgaben des IT Service Continuity Managements verbunden, jedoch ist es zur Erreichung der Ziele der Informationssicherheit notwendig, genau zu unterscheiden, welche Rolle das Security Management während der Gestaltung und Durchführung sowie während der Prüfung spielt.

Im Folgenden sind die wichtigsten Aufgaben beschrieben, die das Security Management im IT Service Continuity Prozess wahrnimmt.

In der Initiierungsphase muss durch das Security Management genau geprüft werden, ob die Aussagen der ITSC-Policy gegen die Sicherheitsziele verstoßen. Außerdem müssen hier die Regeln definiert werden, die während eines Notfalles in Bezug auf die Sicherheitsziele gelten, da dieses ebenfalls durch die Unternehmensleitung mitgetragen werden muss, also quasi die Notstandgesetze der Informationsverarbeitung.

Während der Anforderungsphase arbeiten die Prozesse eng zusammen, da beide auf Basis der aktuellen Assets eine Risikoanalyse durchführen müssen. Hinzukommende Assets, wie zum Beispiel die Battle-Box, müssen hier ebenfalls schon betrachtet werden.

Die Strategiephase wird durch eine Prüfung der gewählten Strategie daraufhin begleitet, ob diese mit den Sicherheitszielen im Einklang stehen.

In der Implementierungsphase leistet das Security Management organisatorische Unterstützung, in dem es dauerhafter Bestandteil der Krisenorganisation ist. Außerdem definiert es Verfahren, wie beispielsweise die Battle-Box zu schützen ist oder welche Kommunikationsregeln während eines Notfalls zu beachten sind. Kennzahlen, die während eines Notfalles als Indikator für die Informationssicherheit dienen sollen, müssen ebenfalls definiert und eingeführt werden. Durch das IT Service Continuity Management beschriebene Verfahren müssen durch das Security Management geprüft und freigegeben werden.

Das operative Management wird durch Definition der Schulungsinhalte unterstützt, die Anwender für Sicherheitsanforderungen und Verfahren während eines Notfalls sensibilisieren. Darüber hinaus begleitet das Security Management die regelmäßigen Notfalltests, um die Verfahren zu prüfen.

3.4.6 Finance Management for IT Services

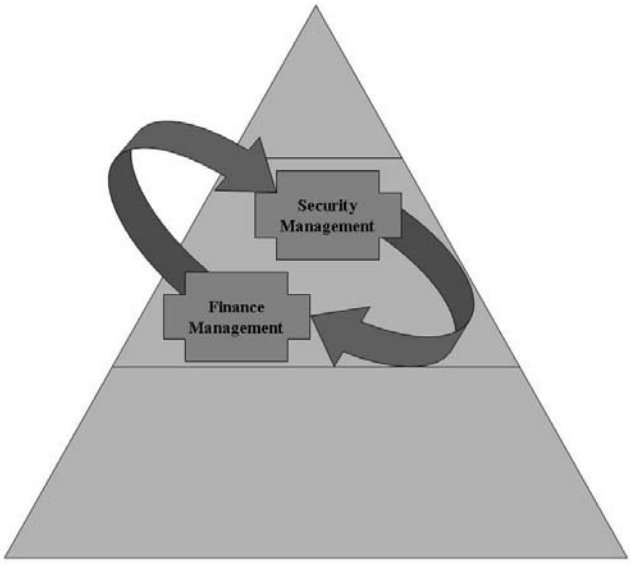


Abbildung 16: Security & Finance Management

Das Finance Management for IT Services wird in einigen Publikationen auch Financial Management and Costing genannt.

Damit zielt es auf die drei Hauptaufgaben, die das Finance Management for IT Services hat, nämlich dem

- Budgeting, der Zuordnung von Mitteln zu bestimmten Projekten und IT-Services, auch Finanzplanung genannt,
- Accounting, der Ermittlung der Kosten bezogen auf Verursacher und IT-Service und
- Charging, der Abrechnung der in Anspruch genommenen und durch das Accounting festgestellten Leistungen.

Diese drei Schritte durchläuft jeder IT-Service, der durch den IT-Dienstleister geplant, implementiert und schließlich erbracht wird. Zum Zwecke der Ermittlung, welche IT-Services oder Projekte implementiert oder durchgeführt werden sollen, werden zusätzlich noch der Return on Investment sowie die Total Cost of Ownership errechnet.

Der Return on Investment (RoI) drückt aus, nach wie langer Zeit sich eine Investition gerechnet und seine Kosten wieder eingebracht hat.

Die Rentabilität eines IT Service wird in der erhöhten Effizienz beziehungsweise in einer erweiterten Funktionalität gesehen, die beispielsweise mehreren Benutzern gleichzeitig einen Zugriff auf einen IT-Service gestattet. Das RoI ist ein Kriterium für Investitionsentscheidungen.

Für das Security Management ist der RoI schwer zu berechnen, da es hier keine allgemeingültigen und damit vergleichbaren Verfahren gibt. Hier sollte die Frage im Vordergrund stehen, welche Risiken ohne die notwendige Informationssicherheit bestehen, die hier dem IT Service einen RoI ermöglicht.

Die Total Cost of Ownership (TCO) beschreibt alle Kosten, die für die Planung, den Betrieb und die Beendigung eines IT-Services entstehen, also den IT-Service Lifecycle.

Üblicherweise geht man von einer Verteilung von 30% Kapitalkosten aus (Kauf, Implementierung, Lizenzen) und 70% Kosten, um den IT Service zu betreiben (Wartung, Betrieb, Anwendersupport). Dies zeigt die besondere Bedeutung einer guten Finanzplanung von IT-Services. In Bezug auf das Security Management gilt, je sicherer und beherrschbarer ein IT-Service ist, umso geringer ist sein TCO.

Das Security Management muss besonders in der Planungsphase eines IT-Service eine enge Abstimmung mit dem Finance Management vornehmen, damit es das Budget und damit die Möglichkeiten erhält, die Sicherheitsziele sicherzustellen. Ohne die benötigten finanziellen Mittel kann das Security Management keine Maßnahmen ergreifen, um Bedrohungen für die IS zu begegnen, aber ebenso wenig können dann Analysen durchgeführt

werden. Die Ausstattung des Security Managements ist zudem ein guter Gradmesser, welche Unterstützung ein Unternehmen diesem Thema tatsächlich beimisst. Hohe Budgets bedeuten nicht zwangsläufig einen hohen Grad an Unterstützung, aber niedrige Budgets geben einen deutlichen Indikator, dass die Unternehmensleitung dem Thema Security Management nicht die notwendige Beachtung schenkt.

Beim Budgeting muss darauf geachtet werden, dass die Maßnahmen einberechnet sind, die aufgrund der Klassifikation notwendig sind, um die Sicherheitsziele zu gewährleisten. Dieses bedeutet, dass die Maßnahmen bereits in einem Service-Katalog für Security berücksichtigt und mit Kosten hinterlegt worden sind. Eine weitere Möglichkeit ist, einen festen prozentualen Anteil als Kosten für die IS einzukalkulieren. Dieser sollte dann über mehrere IT-Services ermittelt werden und repräsentativ sein, da er ansonsten angezweifelt werden kann. Gerade in Budgetverhandlungen ist es wichtig, jede Maßnahme immer auf die Sicherheitsziele beziehen zu können, so dass die IS nicht als Selbstzweck dargestellt werden kann.

Das Accounting soll feststellen, welche IT-Services in welchem Umfang durch die Anwender in Anspruch genommen worden sind. Dazu muss definiert werden, wann ein IT-Service als geleistet angesehen wird und welchen Einfluss beispielsweise Security Incidents auf das Accounting haben, die für eine längere Zeit zum Ausfall des zentralen Netzwerkknotens führen oder zu anderen Störungen der Leistungserbringung. Hier muss die zentrale Frage beantwortet werden, wer das Risiko von Security Incidents trägt –IT-Dienstleister oder Kunde. Dieses muss im SLA geregelt sein, das auch für das Accounting die verbindlichen Regeln aufstellt.

Durch das Charging wird die tatsächliche Verrechnung mit dem Kunden vorgenommen. Da es immer häufiger Bonus und Malus Regelungen gibt, bei denen der Kunde zum Beispiel weniger zahlen muss, wenn ein gewisser Grad des IT-Services nicht erreicht worden ist, ist es hier besonders wichtig, zu belastbaren und richtigen Werten zu kommen. Das Security Management muss hier für die Integrität der erhobenen Daten sorgen, die relevant für Bonus oder Malus Zahlungen sind. Dieses kann durch das gesicherte Abspeichern der Protokolldateien erreicht werden.

3.5 Security Management auf der operativen Ebene

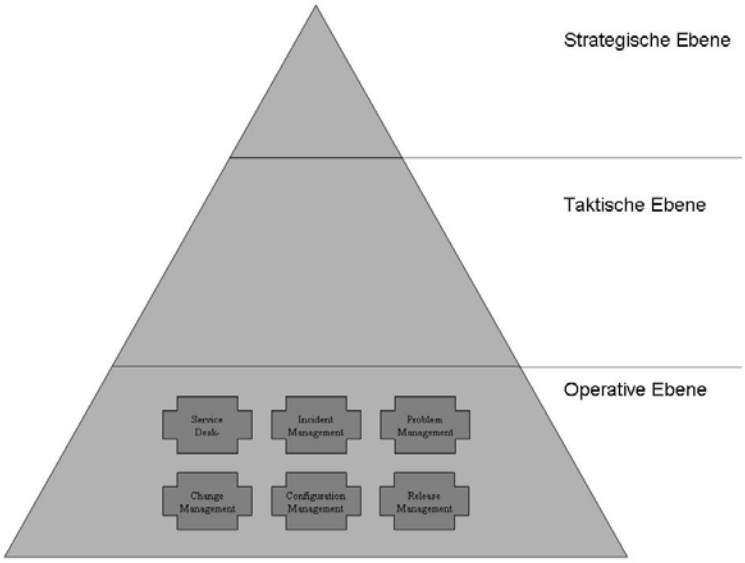


Abbildung 17: Security Management auf der operativen Ebene

Die operative Ebene bei ITIL wird durch den Service Support beschrieben. Hier sind die Verfahren und Prozesse definiert, die für die direkte Leistungserbringung von IT-Services nötig sind.

- Service Desk
- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Release Management

Im folgenden Kapitel werden die Schnittstellen zwischen den Prozessen des Service Support und dem Security Management beschrieben.

3.5.1 Service Desk

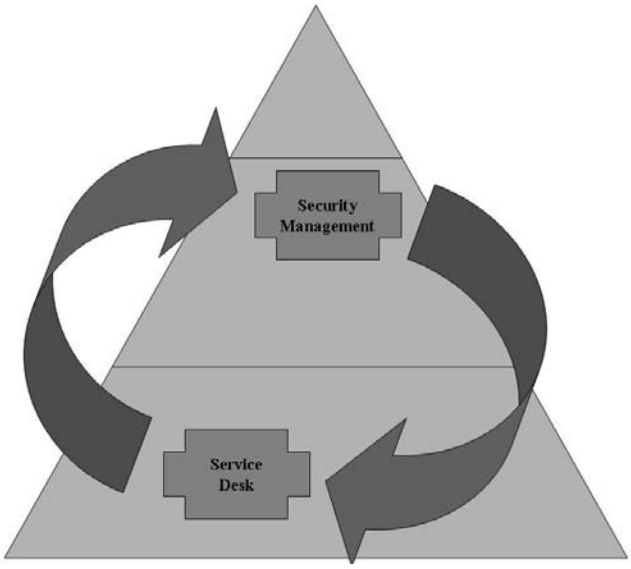


Abbildung 18: Security Management & Service Desk

Die Aufgabe des Service Desk ist die Aufnahme von jeglicher Kommunikation zwischen Anwendern und der IT-Organisation. Dazu zählen

- Störungen
- Anfragen
- Wünsche
- Aufträge
- Service Requests

Da der Service Desk die einzige Anlaufstelle für Anwender darstellt, hat er häufig noch die Funktion eines Kummerkastens. Deshalb sind die Mitarbeiter des Service Desk häufig gut ausgebildete Kommunikationsexperten.

Das Ziel des Service Desk ist eine einfache Kommunikation der Anwender mit der IT-Organisation.

Da Strukturen, die auf ITIL basieren, in der Regel in bestehende Unternehmensstrukturen eingeführt werden müssen, hat der Service Desk eine zentrale Bedeutung für den Erfolg eines ITIL Projektes. Vorhandene kollegiale Beziehungen zwischen Fachbereichen und IT-Spezialisten führen über lange Jahre zu bestimmten Kommunikationsstrukturen, von der Hardwarebeschaffung bis zur Störungsmeldung.

Diese, in ITIL Büchern gerne „Hey, Joe"-Effekt genannten Gewohnheiten, führen zu einem Diversifizieren der Kommunikation und damit zu einer fehlenden Transparenz.

Aus diesem Grund ist es für den Service Desk von strategischer Bedeutung, dass dieser leicht erreichbar ist und dem Anwender dort auch geholfen wird.

Der Service Desk wird in den meisten Unternehmen durch das Incident Management wahrgenommen. Daher werden die Aufgaben und Ziele des Security Managements in dem Abschnitt über das Incident Management dargestellt.

Eine Störung (engl. Incident) ist ein Ereignis, das nicht zum planmäßigen Betrieb eines IT-Services gehört und das als tatsächliche oder mögliche Auswirkung eine Minderung der Service-Qualität verursacht oder zum Ausfall des Service führt.

3.5.2 Incident Management

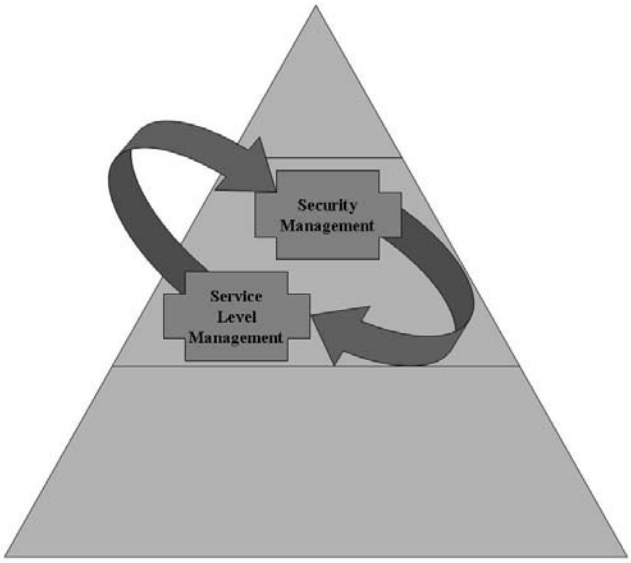


Abbildung 19: Security & Incident Management

Die Aufgabe des Incident Managements ist die gesamtheitliche Verwaltung aller Störungen.

Durch die Registrierung wird die systematische Aufnahme von Störungen gewährleistet und an einer definierten Stelle gespeichert. In den Zeiten vor der Informationstechnologie wurden Register in Büchern geführt, die aufgrund der schlechten Kopierbarkeit zentral verwaltet wurden. Durch die immer stärker verteilte Datenhaltung wird dieses für moderne Verfahren, die auf Informationstechnologie beruhen, erschwert. Die meisten Unternehmen setzen deshalb zur Verwaltung von Störungen Werkzeuge ein, wie zum Beispiel Trouble Ticket Systeme. Diese haben den großen Vorteil, dass sie noch viele weitere Aufgaben darstellen können und häufig bereits ITIL Prozesse bei der Entwicklung berücksichtigt worden sind.

Eine Klassifizierung der Störung wird vorgenommen, indem Art und Status der Störung erfasst werden. Aus der Klassifizierung sollte ersichtlich sein, welche Sicherheitsziele betroffen sind.

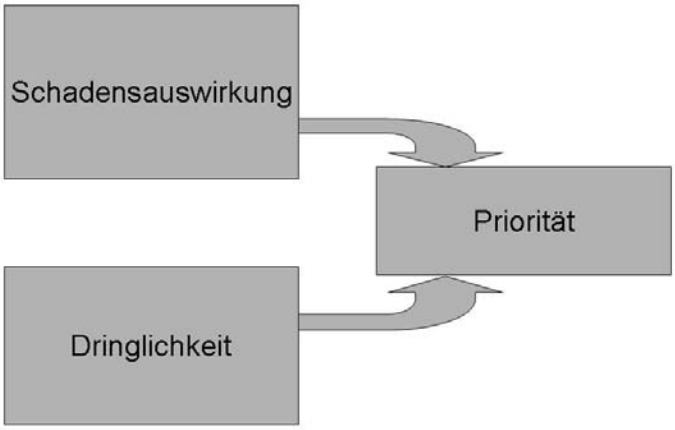


Abbildung 20: Priorisierung

Die Priorität ist ein Entscheidungskriterium, welches aus der möglichen Schadensauswirkung und der Dringlichkeit ermittelt wird.

Durch die Schadensauswirkung wird die mögliche Auswirkung auf die IT-Services beschrieben. Die Schadensauswirkung wird im Rahmen einer Risikoanalyse untersucht.

Die Dringlichkeit beschreibt die maximale Zeit, nach der ein Sicherheitsziel wieder erreicht werden muss. Bei Notfällen ist dieses zum Beispiel die Maximale Wiederanlaufzeit.

Eine Analyse der Störung beginnt mit der Prüfung, ob es sich um eine bereits bekannte Störung handelt. Falls dieses zutrifft, wird die definierte Lösung gewählt, beziehungsweise der vorgeschlagene Workaround. Wenn eine Störung nicht bekannt ist und auch keine schnelle Lösung dafür gefunden werden kann, wird die Störung zu dem nächsten Support-Team eskaliert. Die Zusammensetzung der Support-Teams wird häufig mit dem n-Level Konzept beschrieben, wobei die Gruppe, die für das Incident Management verantwortlich ist, den First Level Support darstellt.

Die Verfolgung einer Störung wird notwendig, wenn diese nicht gleich durch das Incident Management gelöst werden kann, sondern erst eskaliert werden muss. Auch bei Lösungen, die einen zeitlichen Vorlauf benötigen, zum Beispiel durch Programmierarbeiten, muss das Incident Management den Status der Lösung verfolgen. Das Incident Management ist in jedem Fall der „Eigner" einer Störung.

Ein Abschluss einer Störung bedeutet, dass das Incident Management eine Störung als gelöst an den Service Desk zurückgibt, der dann den Anwender darüber informiert.

Das Incident Management ist der Hauptlieferant für das Security Management, da jede Störung auch eine Störung der Informationssicherheit (Security Incident) sein kann. Aus der Sicht des Incident Managements gibt es keinen Unterschied zwischen einer „normalen" Störung und einem Security Incident. Lediglich die Art und Weise, in der mit der Störung verfahren wird, unterscheidet sich, sobald eine Störung als Security Incident klassifiziert worden ist.

Um die Nachverfolgbarkeit der Störungen der Informationssicherheit zu gewährleisten und damit auch den aktuellen Status sowie Trends für die Zukunft abzuleiten, müssen durch das Incident Management bestimmte Anforderungen an die Dokumentation von Störungen erfüllt werden. Demnach muss eine Störung folgendermaßen dokumentiert sein:

- Eindeutige Störungsnummer (mit Datum und Uhrzeit der Meldung)
- Wann ist die Störung aufgetreten? (Uhrzeit und Datum)
- Wo ist die Störung aufgetreten? (Standort, Abteilung, System, Netzwerk)
- Wer hat die Störung gemeldet?
- Störungsbezeichnung aus Schlagwortkatalog
- Genaue Beschreibung der Störung
- Entstandener Schaden (auch geschätzt)
- Priorität
- Lösung

Die Aufgabe des Incident Managements ist es, Security Incidents so schnell wie möglich zu identifizieren. Nicht jeder Security Incident wird allerdings durch das Incident Management gemeldet, da automatisch erzeugte Alarmmeldung oder Auditergebnisse direkt durch das Security Management erhoben werden.

Wenn Zweifel bestehen, ob es sich um einen Security Incident handelt, sollte diese Störung immer wie ein Security Incident behandelt werden.

Eine Störung der Informationssicherheit (engl. Security Incident) ist ein Ereignis, das die Verfügbarkeit, die Integrität oder die Vertraulichkeit beim Betrieb eines IT-Services verletzt und das als tatsächliche oder mögliche Auswirkung eine Minderung der Sicherheitsziele verursacht. Im ITIL Kontext sind diese Sicherheitsziele in den SLA festgelegt worden.

In einem SLA sollten IS-Mindeststandards (Security Baseline) beschrieben sein. Sobald diese nicht mehr eingehalten werden können, liegt ebenfalls ein Security Incident vor.

Beispiele für Security Incidents sind:

- Vertraulichkeit:
  - Notebookdiebstahl
  - PDA-Verlust
  - Verlust mobiler Speicher (USB-Sticks)
  - Hacking
  - Auffinden von Ausdrucken mit vertraulichem Inhalt im Papiermüll

- Verfügbarkeit:
  - Ausfall Netzwerk
  - Absturz einer Festplatte
  - Fehlerhaftes Backup
  - Fehlerhafter Restore

- Integrität:
  - MalWare
  - Digitaler Replay-Angriff
  - Zugriff auf Internet-Anwendung unter Umgehung der Plausibilitätsprüfungen

Einige Security Incidents betreffen mehrere Sicherheitsziele, wie zum Beispiel der Verlust eines PDAs, der einerseits nicht mehr für die Arbeit vorhanden ist (Verfügbarkeit), aber gleichzeitig auch Dritten unbefugten Zugriff auf Informationen ermöglicht (Vertraulichkeit). So können kleine Störungen eine große Auswirkung haben.

Sobald ein Security Incident identifiziert worden ist, muss schnell das richtige Verfahren angewandt werden. Hier ist entscheidend, dass alle betroffenen Konfigurationselemente (CI) identifiziert werden, da höher klassifizierte Konfigurationselemente (CI) eventuell auch ein anderes Verfahren fordern, nachdem mit einer Störung der Informationssicherheit umgegangen werden muss.

Da es zu sehr unterschiedlichen Störungen der Informationssicherheit kommen kann, sollte für das Incident Management für eine repräsentative Anzahl von Security Incidents beschrieben sein, wie mit diesen umgegangen werden muss. Diese Verfahrensbeschreibungen sollten Teil der SLA sein.

Ebenso sollte in einem SLA geregelt sein, wann welche Berichte an den Fachbereich oder den Kunden erfolgen müssen.

Das Security Management hat an erster Stelle dafür zu sorgen, dass ein Security Incident beseitigt wird. Jeder Security Incident sollte aber auch dazu führen, dass präventive Maßnahmen aufgesetzt werden, die eine weitere Störung der Informationssicherheit zukünftig verhindern.

Security Incidents vermitteln bei betroffenen Anwendern häufig die große Befürchtung, dass ihr Verhalten zu dieser Störung geführt hat. Die häufig unberechtigte Angst, dass durch ihre Schuld dem Unternehmen ein Schaden entstanden sein könnte hindert viele Anwender daran, die Störung so schnell wie möglich zu melden.

Viele Anwender verstehen daher auch das Security Management als eine Art Polizei, die das Fehlverhalten von Anwendern bestraft. Diesem Gerücht muss durch geeignete Schulungsmaßnahmen begegnet werden.

In vielen Projekten hat es sich als positiv erwiesen, auch anonyme Störungsmeldungen entgegen zu nehmen, da hier die Hemmschwelle herabgesetzt wird. Dieses sollte natürlich die Ausnahme bleiben, da der Anwender für die Aufklärung von Security Incidents wichtige Hinweise liefern kann.

Darüber hinaus sollte in einem IS-Handbuch das Verfahren beschrieben werden, nach dem Security Incidents zu melden sind.

3.5.3 Problem Management

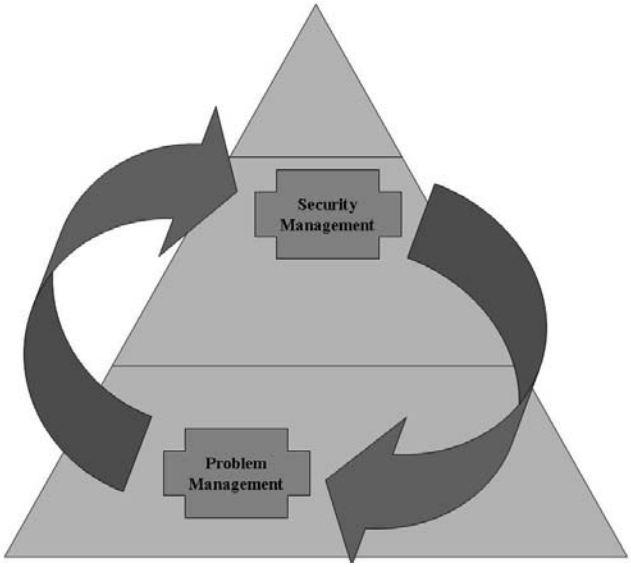


Abbildung 21: Security & Problem Management

Das Problem Management beginnt dort, wo das Incident Management aufhört. Durch das Incident Management werden die Gründe, die zu einer Störung führen, nicht erforscht. Daher kann sich eine Störung wiederholen, wenn die Ursache erneut auftritt.

Die Aufgabe des Problem Managements ist es, die Ursachen für bereits aufgetretene Störungen reaktiv und für zukünftig mögliche Störungen proaktiv zu analysieren.

Ein Problem ist ein Fehler, dessen Ursache noch nicht bekannt ist.

Sobald die Ursache eines Problems erkannt worden ist, wird es damit zu einem bekannten Fehler. Häufig schließt sich hier ein Änderungsantrag für das Change Management an, ein Request for Change (RfC).

Während beim Incident Management die Schnelligkeit der Lösung maßgebend ist, zielt das Problem Management auf eine nachhaltige Identifizierung und Ausschaltung der Ursache ab.

Das Problem Management analysiert aufgrund der Fülle von Störungen, die täglich auftreten, meist nur die schweren Fehler sowie die Fehler, die immer wieder auftreten.

Nachfolgend sind Beispiele für typische Probleme aufgeführt:

- Eine Sicherheitsüberprüfung von außen (Pentest[5]) hat ergeben, dass die Infrastruktur Schwachstellen aufweist
- Eine Störung führt dazu, dass die SLAs mit dem Kunden nicht eingehalten werden können.

Die Aufgaben des Problem Managements in Bezug auf die Analyse von Security Incidents sind sehr wichtig, da an dieser Stelle so genannte Root Cause Analysen durchgeführt werden, durch die Ursachen von unerklärlichen Sicherheitsproblemen aufgeklärt werden können.

Bezogen auf das Security Management sind folgende kritische Erfolgsfaktoren zu nennen:

- Ein RfC, der durch das Problem Management erzeugt wird, darf keinen neuen Fehler beinhalten, der zu Security Incidents führt
- Änderungen müssen sinnvoll und durchgängig getestet werden. Hier ist es besonders wichtig, dass die Anforderungen an die IS in Form von Testverfahren beschrieben sind. Nur dadurch kann eine Aussage getroffen werden, ob eine Änderung erfolgreich war oder nicht. Tests von Änderungen sollten alle relevante Systeme berücksichtigen um sicherzustellen, dass nicht an anderer Stelle Lücken entstehen
- Die Analyse muss durch Sicherheitsspezialisten unterstützt werden.
- Da die Analyse von CIs Kenntnisse über bestehende Sicherheitslücken bringen kann, sollten nur wenige Personen an der Analyse beteiligt sein
- Eine Veröffentlichung der Lücken sollte erst nach dem Abschalten der Schwachstelle geschehen

[5] Kurzform für Penetrationstest; Versuch, ein Unternehmen mit den Mitteln eines Hackers anzugreifen

- Häufig fehlen bei Problem Management Experten, die für Analysen der IS in unterschiedlichen Disziplinen nötig sind, um tiefgreifende Root Cause Analysen durchzuführen. Andererseits werden Experten stark in eine Vielzahl von neuen Projekten eingebunden, aus denen diese nicht heraus können, da in den Projekten sonst Implementierungsfehler stattfinden, die später durch das Problem Management untersucht werden müssen.

3.5.4 Change Management

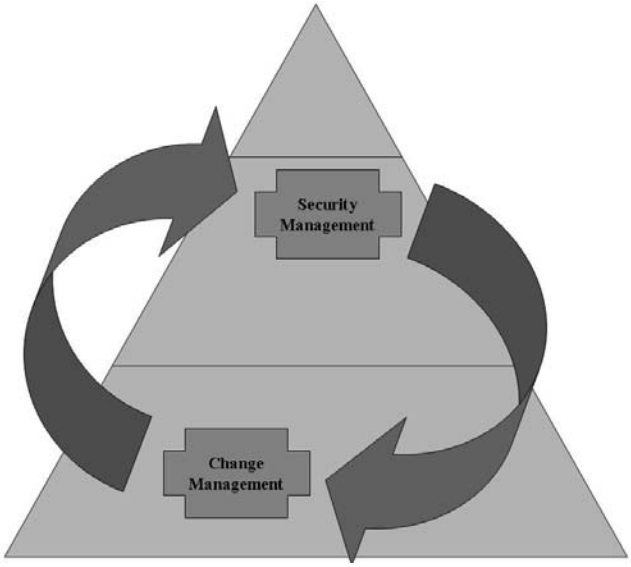


Abbildung 22: Security & Change Management

Das Change Management stellt die zentrale Instanz im ITIL Prozessmodel dar. Durch diesen Prozess laufen alle Änderungen (Change) an der IT-Infrastruktur, also an allen Systemen, Applikationen und Netzwerken.

Die wichtigste Aufgabe des Change Management ist es, einen Überblick zu behalten.

Eine zweite Aufgabe ist die Kontrolle bezüglich der sauberen Umsetzung, sowohl unter Kosten-, wie auch unter Technikaspekten.

Kontrolle bedeutet hier, dass das Change Management die Bereiche steuert, die Tests durchführen oder, wie im Falle des Release Management, den Prozess steuert, der das operative Rollout durchführt.

Ein Rollout ist die Einführung eines neuen oder geänderten Releases in die IT-Infrastruktur.

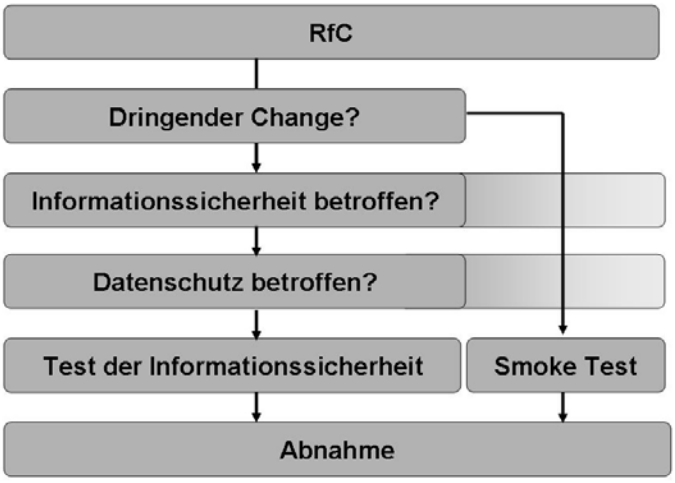


Abbildung 23: Abnahme von RfCs

Das Change Management bewertet RfCs und muss in einer ersten Analyse feststellen, ob es sich um einen dringenden Change handelt, weil z.B. die Erfüllung der Servicevereinbarung nicht gewährleistet ist. Bei dringenden Changes wird ein verkürztes Verfahren durchlaufen, das aber die Stufen im Wesentlichen beinhaltet.

In einem zweiten Schritt wird auf Basis einer Entscheidungsmatrix festgestellt, ob ein Change Auswirkungen auf die Informationssicherheit hat. Die Prüfung nimmt das Security Management vor.

Wenn ein Change die Informationssicherheit betrifft, muss untersucht werden, ob die Sicherheitsziele aus dem SLA durch den Change berührt werden und nach diesem noch erreichbar sind. Der Security Manager muss einen Change ablehnen, der die Erreichung der Sicherheitsziele verhindert.

Bei einer Ablehnung wird ein Änderungsgremium (CAB = Change Advisory Board) einberufen, das eine Lösung finden muss.

Für erfolgreiche RfCs, welche die IS betreffen, müssen durch das Security Management die Abnahmekriterien definiert werden. Bei dringenden Changes wird dieses Verfahren ebenfalls durchlaufen, nur werden die Abnahmekriterien an die Dringlichkeit angepasst, und so genannte Smoke Tests müssen definiert werden, um einen qualifizierten Hinweis zu bekommen, ob der Change die Sicherheitsziele erreicht hat. Der Begriff Smoke Test bildet eine Analogie zum Feuermachen, wo man sich auf dem richtigen Weg weiß, wenn der Rauch sichtbar wird.

In vielen deutschen und österreichischen Unternehmen wird bereits heute im Change Management geprüft, ob ein Change den Datenschutz betrifft.

Wenn die Sicherheitsziele positiv geprüft worden sind, kann aus Sicht des Security Managers der Change freigegeben werden.

Bei kleineren Änderungen wird diese Freigabe direkt durch den Change Manager erteilt. Bei größeren Änderungen entscheidet das CAB über die Freigabe eines Changes. Der Security Manager ist darüber hinaus ständiges Mitglied im CAB.

Die Sicherheitsziele betreffen die meisten Changes, daher sollte jeder Antragsteller eines RfC die IS im Auge behalten. Projekte, bei denen das Security Management eingeführt worden ist, haben gezeigt, dass am Anfang relativ viel Aufwand durch den Security Manager erbracht werden muss, um RfCs so zu gestalten, dass die Sicherheitsziele eingehalten werden können. Im Laufe der Zeit wird dieser Aufwand immer geringer.

Bei einem Rollout muss durch Tests sichergestellt werden, dass die Sicherheitsziele eingehalten worden sind. Hierzu muss ein erweiterter Testansatz gewählt werden, der nicht nur die Korrektheit einer bestimmten Funktion feststellt, sondern auch das Fehlen unerwünschter Nebenwirkungen, wie zum Beispiel Hintertüren in Software-Applikationen.

3.5.5 Configuration Management

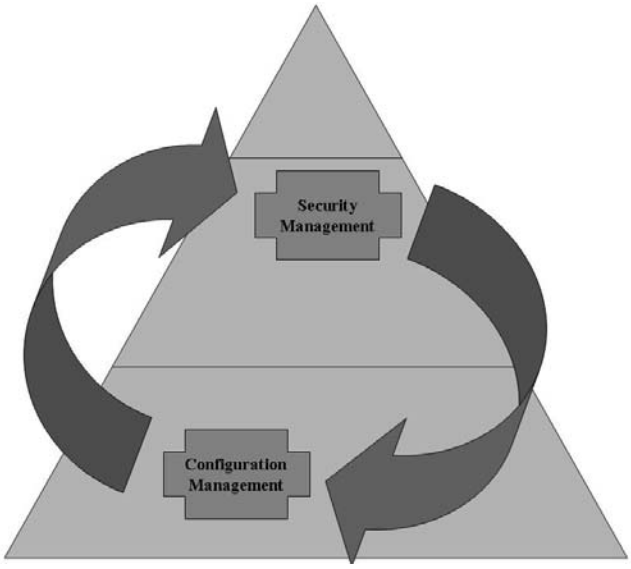


Abbildung 24: Security & Configuration Management

Das Configuration Management wird immer häufiger auch Configuration & Asset Management genannt, da die Service-orientierte ITIL-Sicht auf die Konfigurationselemente (CI; Configuration Items) dieselbe Zielrichtung hat wie das klassische Asset Management, das sich um die kaufmännischen Werte der IT-Infrastruktur kümmert.

Unter Configuration Items (CI) werden IT-Systeme, wie zum Beispiel Server und Arbeitsplatz-PC, Peripheriegeräte, wie zum Beispiel Drucker und Scanner, aber auch Handbücher, Netzwerkkomponenten und Datenträger verstanden. Diese werden in der Configuration Management Database (CMDB) gespeichert.

Die Hauptaufgabe des Configuration Management ist es eine Übersicht über alle CIs einer IT-Infrastruktur herzustellen, diese zu erhalten und die der Abhängigkeiten der CIs untereinander sichtbar zu machen. Dazu wird durch das Configuration Management ein logisches Modell aufgebaut, in dem alle CIs in dem jeweils benötigten Detaillierungsgrad festgehalten werden.

Beispielsweise muss zum Installieren einer aktiven Netzwerkkomponente der ausführliche Installationsvorgang beschrieben sein. Zum Anschließen einer Maus ist dieses vermutlich nicht notwendig.

Dieses logische Modell wird in der CMDB implementiert, um einerseits die Datenmengen beherrschbar zu machen, aber auch um anderen Prozessen einfachen Zugang zu den Informationen zu geben.

Das Configuration Management ist aus Sicht des Security Managements der zentrale Prozess innerhalb des Service Support, da er die Grundlage dazu bildet, dass Anforderungen aus den Geschäftsprozessen hinsichtlich seiner Relevanz zur IS in alle Prozesse des IT-Betriebes einfliessen, und zwar durch Klassifikation.

In der CMDB muss jede CI klassifiziert werden. Die Klassifikation leitet sich direkt aus der Anforderung eines Geschäftsprozesses ab.

Da nur der Besitzer eines Geschäftsprozesses die Risiken und Auswirkungen für seinen Geschäftsprozess kennt, muss er das Maß der IS vorgeben, das benötigt wird.

Die Klassifikation drückt genau diese Anforderungen aus, in dem die Abhängigkeiten zwischen Geschäftsprozessen, CIs und Informationen bewertet werden.

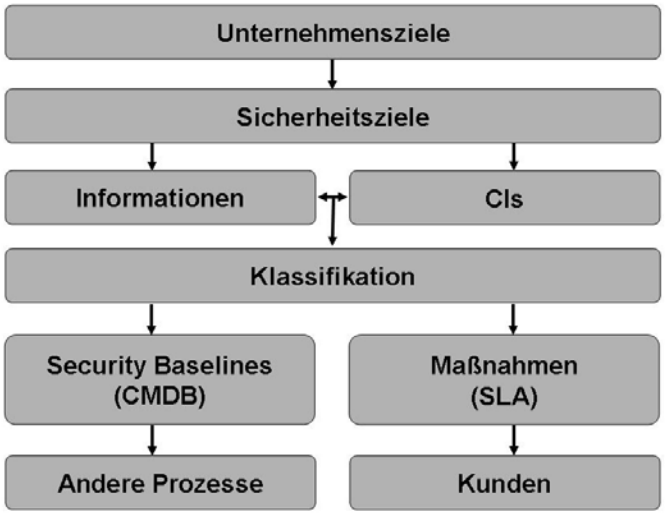


Abbildung 25: Verbreitung der Sicherheitsziele

Die IT-Organisation definiert die Maßnahmen und Verfahren, die ergriffen werden müssen, wenn CIs eine bestimmte Klassifikation erhalten.

Ein Beispiel ist die Übertragung von wichtigen Unternehmensinformationen per E-Mail. Die Klassifikation in Bezug auf Vertraulichkeit ist in diesem Beispiel als hoch eingestuft. Die Maßnahme, die man ergreifen könnte, ist die Verschlüsselung der E-Mail.

Eine Klassifikation wird hinsichtlich der drei Hauptsicherheitsziele vorgenommen, nämlich

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität.

Nachfolgend wird eine Übersicht über mögliche Klassifizierungssysteme gegeben.

Es wird an dieser Stelle explizit darauf hingewiesen, dass alle Verfahren dann am besten angenommen werden, wenn diese einfach zu benutzen sind.

Es kommt auch nicht nur darauf an, dass eine 100%ige Klassifizierung aller CIs vorgenommen wird, sondern dass überhaupt Klassifikationen durchgeführt werden. Durch die stetig wachsende Datenmenge im Unternehmen wird sonst eine Beherrschbarkeit nicht mehr gewährleistet.

Vertraulichkeit

Klassifikation	Kriterium
Streng geheim	Beispielsweise Betriebsgeheimnisse & Formeln, Datenschutz, besondere Gesetze, Kalkulationen
Geheim	Interne Infos (z.B. Preislisten), Besprechungsnotizen, unfertige Dokumente
Eingeschränkt	Alle Informationen, die durch Dritte gesehen werden können, aber nicht für diese bestimmt sind
Öffentlich	Öffentlich zugänglich (Presse, Marketing, Web-Seite)

Tabelle 1: Klassifikation Vertraulichkeit

Verfügbarkeit

Klassifikation	Kriterium
Hoch	Häufig werden hier Prozentzahlen genannt. Wichtig ist, das klar formuliert wird, welche Bezugsgröße 100% ist und welche Ausnahmen gelten (Wartung, Naturkatastrophen, …) Diese muss zu der Schadensauswirkung in Beziehung gesetzte werden.
Mittel	
Niedrig	
Keine	Falls ein CI keine Anforderung an die Verfügbarkeit hat, kann diese wahrscheinlich abgeschaltet werden. Daher wird diese Stufe nie benutzt.

Tabelle 2: Klassifikation Verfügbarkeit

Integrität

Bei der Klassifikation von CIs hinsichtlich der Integrität muss die größte Sorgfalt angewandt werden, da schwer zu definieren ist, wie viele falsche Daten eine Datenbank verträgt oder wie viele Verbindungsfehler in einem Netzwerk vorkommen dürfen. Leider fehlt dazu häufig die Kenntnis, welcher Grad an Integrität heute erreicht wird.

Es wird daher in der Regel eine Baseline Integrität definiert, die für alle CIs als Vorgabe besteht. Sollte ein CI höhere Anforderungen an die Integrität besitzen, wird diese entsprechend definiert. Daher ist das Klassifikationssystem hier sinnvollerweise zweistufig.

Klassifikation	Kriterium
Erweiterte Integrität	Individuelle Anforderung, beispielsweise Computertelefonie (VoIP), elektronischer Wertpapierhandel, …
Baseline Integrität	Beispielsweise Anzahl akzeptierter Verbindungsabbrüche, Fehlerhafte Datensätze, …

Tabelle 3: Klassifikation Integrität

Neben der Klassifikation hat das Configuration Management noch folgende weiteren Schnittstellen zu dem Security Management:

- Durch eine aktuelle CMDB wird die Analyse von Schwachstellen und sicherheitsrelevanten Interaktionen zwischen CIs erst ermöglicht.
- Da ein Incident und ein RfC nur für bekannte CIs aufgegeben werden können, wird die Abdeckung der CMDB über alle tatsächlich eingesetzten CIs immer größer, da jeder Change und jeder Incident dazu führt, dass noch nicht registrierte CIs in die CMDB aufgenommen werden. Durch die wachsende Übersicht nehmen die Tretminen in der IT-Infrastruktur ab, die als nicht erkannte Verbindungen und Funktionen, oder sogar als nicht registrierte Hardwarekom-

ponenten, wie zum Beispiel ein aktives Modem in einem Notebook, existieren.

- Das Asset Management unterstützt die Verwaltung der Lizenzen (Digital Right Management, DRM), da beispielsweise bei CPU-basierten Lizenzen alle genutzten Systeme bekannt sein müssen.
- Ein funktionierendes Configuration Management erleichtert Analysen von Security Incidents, da hier die Historie aller CIs mit allen Changes revisionssicher gespeichert ist.

3.5.6 Release Management

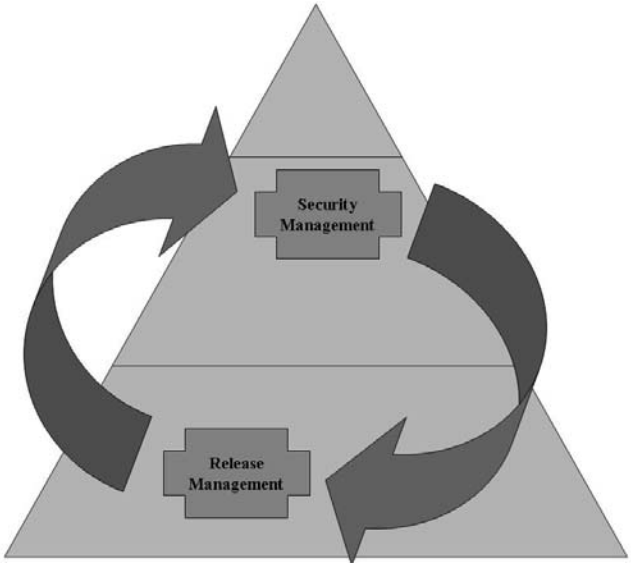


Abbildung 26: Security & Release Management

Während das Change Management die Verantwortung für alle Änderungen hat, die in die IT-Infrastruktur eingehen, steuert das Release Management die tatsächliche Umsetzung der Änderungen.

Der Input für den Prozess Release Management ist ein genehmigter Change.

Das Release Management definiert die Release-Grundsätze, die beschreiben, welche Voraussetzungen ein Release erfüllen muss um diese in die IT-Infrastruktur einführen zu können.

Durch die Definition von Baselines werden die Releases standardisiert, so dass sich bei einem funktionierenden Release Management nach und nach ein hohes Maß an Standardisierung der IT-Infrastruktur einstellt.

Die Ziele des Release Managements sind

- Effektivität,
- Sicherheit und
- Nachvollziehbarkeit bei Änderungen an der IT-Infrastruktur.

Ein zentraler Punkt ist auch hier das Testen von Releases. Das Release Management stellt durch geeignete Verfahren sicher, dass die Release-Grundsätze durch eine Änderung eingehalten werden.

Das Release Management hat hier im Besonderen die Aufgabe, die unterschiedlichen Releases innerhalb einer IT-Infrastruktur im Gesamtkontext des IT-Betriebes zu betrachten und den Schutz der Produktionssysteme sicherzustellen.

Eine wichtige Forderung der Release Managements ist eine produktionsidentische Testumgebung, auf der die unterschiedlichen Releases in der jeweils zu einem Rollout gültigen Version durchgängig gegeneinander getestet werden können. Diese Durchgängigkeit muss sowohl durch die Testsysteme möglich sein, wie auch durch die Vorhaltung von konsistenten Testdaten.

Das Release Management steuert ferner die Definitive Software Library (DSL), ein Archiv, in der alle genehmigten und aktuellen Softwareversionen vorgehalten werden. Diese DSL ist häufig ein Teil der CMDB.

Ebenso steuert das Release Management den Definitive Hardware Store (DHS), ein Lager, das sämtlich genehmigte Hardwaresysteme und Ersatzteile enthält.

Abschließend koordiniert das Release Management den Schulungsbedarf bei Anwendern sowie den Trainingsbedarf bei IT-Experten.

Die Hauptaufgabe in Bezug auf Informationssicherheit ist, dass IS-Grundsätze definiert und während einer Rollout-Phase sichergestellt werden. Dieses wird durch folgende Aufgaben unterstützt:

Es wird überprüft, ob sich in der IT-Infrastruktur nur genehmigte CIs befinden. Im Softwarebereich werden regelmäßige Scans durchgeführt, um nach installierter unautorisierter Software zu fahnden. Im Hardwareumfeld können solche Scans ebenfalls durchgeführt werden, jedoch hat der Einsatz von mobilen Speichermedien, USB-Sticks oder auch USB-fähigen Digitalkameras so rapide zugenommen, dass jedes Unternehmen heute einen nicht gewollten Zugriff auf einen USB-Anschluss, dem so genannten Podslurping, verhindern sollte. Welche Hardwarekomponenten in der IT-Infrastruktur betrieben werden dürfen, muss in den Release-Grundsätzen geregelt werden.

Da die Kenntnis von Release-Grundsätzen bei Anwendern eher weniger verbreitet ist, aber hier durch die aktive Mitarbeit der Anwender ein hohes Maß an Sicherheit erreicht werden kann, sollten die wichtigsten Verfahrensregeln für Anwender in einer „präsenten“ Form kommuniziert werden.

Durch die Kenntnis der eingesetzten Software-Anwendungen verringert sich die Anzahl unbekannter Schwachstellen in der IT-Infrastruktur deutlich.

Ein Ziel des Release Managements ist, dass nur legale und autorisierte Software-Anwendungen im Rahmen der Lizenzbestimmungen eingesetzt werden darf. Das Thema DRM stellt zukünftig eine der großen Anforderungen an das Security Management dar, weil hier mit großem Schadenspotential zu rechnen ist. Dieses kann hohe finanzielle, sowie Reputationsschäden mit sich bringen, wenn zum Beispiel innerhalb einer IT-Infrastruktur Systeme betrieben werden, auf denen die neuesten Hollywoodfilme in DVD-Qualität gespeichert sind. Ebenso ist eine deutliche Unterlizenzierung von eingesetzten Software-Anwendungen strafbar.

Durch das Testen können Bedrohungen, wie zum Beispiel Mal-Ware oder Hintertüren, gefunden und rechtzeitig abgestellt werden.

Die Gesamtübersicht aller Änderungen hilft dem Security Management eine release-übergreifende Risikobetrachtung darüber anzustellen, ob zum Beispiel durch die Änderung an der Schnittstelle einer Software-Anwendung die Sicherheitsziele noch eingehalten werden können.

Für den integrativen Testansatz ist es besonders wichtig, dass alle Rollouts zentral gesteuert werden, um risikobehaftete Releases zu verschiedenen Zeiten einzuführen.

Die Planung, wie mit einem nicht erfolgreichen Rollout umgegangen wird ist wichtig für die Fragestellung, wie lange der IT-Betrieb durch eine Rollout-Aktivität gestört oder unterbrochen werden darf. Dieses wird in den SLA geregelt. Im einfachsten Falle sollte ein Fallback oder Backout durchgeführt werden.

Ein Fallback ist die Wiederherstellung der vorherigen Releases. Dadurch werden alle Changes, die in einem Release zusammengefast waren, rückgängig gemacht.

Ein Backout ist ein Verfahren, die einzelnen Changes eines Releases schrittweise rückgängig zu machen. Durch ein Backout wird ein neues Release definiert.

In einigen Fällen kann jedoch die Wiederherstellung einer vorherigen Version nicht mehr bewerkstelligt werden, da der so genannte Point-Of-No-Return sehr früh in einer Rollout-Phase liegt und danach beispielsweise die neue Datenbasis mit der alten Version nicht mehr arbeitsfähig ist. Hier müssen die Kriterien klar in Bezug darauf definiert werden, wann beispielsweise Produktionsdaten in eine neue Version einfließen dürfen (dadurch erreicht man eine Verschiebung des Point-Of-No-Return nach hinten), oder wann ein Notfall ausgerufen werden muss.

4 Security Standards & ITIL

Es gibt eine Anzahl internationaler und nationaler Standards, die sich mit dem Thema IS beschäftigen. An dieser Stelle soll keine vollständige Liste aktueller und gültiger Standards aufgeführt werden, und ebenso keine Empfehlung zur Nutzung des einen oder Vermeidung des anderen Standards gegeben werden. In diesem Kapitel wird eine kurze Übersicht über die Standards gegeben, die für das Thema Security Management relevant und verbreitet sind. Bei der Auswahl eines passenden Standards sind viele Parameter zu berücksichtigen, wie zum Beispiel Branchenzugehörigkeit, internationale Aktivitäten, lokale Gesetzgebungen und Unternehmensorganisation.

4.1 ISO/IEC 17799:2005 (27001:2005)

Es ist eine weit verbreitete Meinung, dass es sich bei der ISO/IEC 17799:2005, beziehungsweise bei der Urfassung des British Standards Institution, nämlich der BS 7799 um einen Standard handelt. In der Tat handelt es sich dabei um Verfahrensregeln (Code of Practice), die es erleichtern, Normen oder staatliche Vorgaben zu erfüllen.

Mit der aktuellen Ausgabe der ISO/IEC 17799:2005 wurde aber auch gleichzeitig ein Standard zum Aufbau eines Information Security Management Systems (ISMS) herausgegeben, der ISO/IEC 27001:2005.

Um die gleiche Bedeutung des Wortes ISO in allen Mitgliedsländern zu gewährleisten, wurde als Namenspatron das Altgriechische Wort Iso = Gleich gewählt. Daher steht ISO nicht, wie häufig vermutet, für „International Standards Organization“.

Die ISO aktualisiert derzeit die Standards für ISMS, so dass eine Reihe von Standards und Verfahrensregeln entsteht, die sämtlich mit der Ziffer 27 beginnen. Die 27er Serie soll wie folgt aussehen:

ISO/IEC 27000	ISMS - Fundamentals und Vocabulary
ISO/IEC 27001	ISMS – Requirements
ISO/IEC 27002	ISM – Code of Practice (derzeit ISO/IEC 17799:2005)
ISO/IEC 27003	ISMS - Implementation Guidance
ISO/IEC 27004	ISM Measurement
ISO/IEC 27004	IS Risk Management

Tabelle 4: ISO/IEC Standards für ISMS

Bis auf den ISO/IEC 27001:2005 und den ISO/IEC 17799:2005 befinden sich alle weiteren Papiere in der Entwicklung. Ob der ISO/IEC 17799 tatsächlich in ISO/IEC 27002 umbenannt werden wird, ist ebenfalls noch nicht entschieden.

ISO/IEC 27001 beschreibt den Aufbau eines ISMS und referenziert im Anhang auf die Maßnahmen, die durch die ISO/IEC 17799 detailliert beschrieben werden.

Der Vorteil des ISO/IEC 17799 ist die internationale Akzeptanz, was global agierenden Unternehmen den Aufbau eines übergreifenden ISMS ermöglicht. Durch die enge Anlehnung von ITIL an ISO/IEC 17799 werden zahlreiche Unternehmen die Maßnahmen, die hier definiert sind, als Grundlage für ihr ISMS umsetzen.

Im Kapitel 5 wird beschrieben, wie die ISO/IEC 17799 in den Security Management Prozess eingebunden werden kann.

4.2 BSI Grundschutzhandbuch

Das BSI Grundschutzhandbuch stellt einen weiteren Best Practice Ansatz dar, wie ein ISMS aufgebaut werden kann. Der große Vorteil des Grundschutzhandbuchs ist die modulare Aufbauweise.

Im Kapitel 2 des Grundschutzhandbuchs wird die Vorgehensweise beschrieben, wie ein Sicherheitsprozess implementiert werden kann und wie ein Sicherheitskonzept erstellt wird. Ebenso werden dort alle Aufgaben des Sicherheitsprozesses definiert.

In den Kapiteln 3 bis 9 werden so genannte Bausteine beschrieben. Die Bausteine aus Kapitel 3 sind übergeordnete Prozesse und Verfahren, wie zum Beispiel Notfallplanung, IT-Sicherheitsmanagement und Organisation. Diese werden dort einmal verbindlich für das Unternehmen definiert. In Kapitel 4 werden die Richtlinien für die Infrastruktur definiert.

Die folgenden Bausteine sind bestimmte Konfigurationen, wie zum Beispiel ein PC unter Windows NT.

Jeder Baustein beschreibt ein Szenario, weist ihm Gefährdungen zu und leitet daraus Maßnahmen ab. Dieses kann mit den Security Baselines aus ITIL verglichen werden.

Der Gefährdungskatalog und der Maßnahmenkatalog sind sehr ausführlich, was bei konsequenter Anwendung einen guten Grundschutz ermöglicht.

Der Vorteil der Ausführlichkeit ist allerdings auch gleichzeitig der größte Feind des Grundschutzhandbuches, da jede Änderung an Systemen und Infrastruktur sofort zu Änderungsaufwand im ISMS führt.

Um diesen Änderungsaufwand beherrschbar zu machen, hat das BSI ein IT-Grundschutz-Tool herausgegeben, das die gesamte ISMS modular abbildet und somit die Verwaltung enorm erleichtert.

Das BSI hat einen hohen Detaillierungsgrad, was sicherlich darauf zurückzuführen ist, dass es für bundesdeutsche Behörden mandatorisch ist, das IT-Grundschutzhandbuch umzusetzen.

Auch in der Wirtschaft wird das IT-Grundschutzhandbuch gut angenommen und verstärkt nachgefragt. In der neuesten Version wurde das IT-Grundschutzhandbuch ISO/IEC 27001:2005 kompatibel gemacht.

4.3 Österreichisches IT-Sicherheitshandbuch

Das Österreichische IT-Sicherheitshandbuch wird von der IKT-Stabstelle des Bundes herausgegeben und ist ein Best Practice Leitfaden zur Erstellung und den Betrieb eines ISMS, mit ausführlichem Maßnahmenteil. Es baut auf dem BSI IT-Grundschutzhandbuch auf, ist jedoch an die Österreichischen Gesetze und Normen angepasst.

4.4 Weitere Standards

Es gibt derart viele Standards, Empfehlungen und Richtlinien für die IT-Security, dass hier nicht alle genannt werden können. Es muss jedoch im Einzelfall immer geprüft werden, ob Branchenverbände verbindliche Vorgaben erstellt haben, oder andere Best Practice Standards besser passen.

In der Regel hat hier jede Interessenvertretung Empfehlungen dazu herausgegeben, wie ein ISMS aufgebaut werden kann. Aber auch Industrie- und Handelskammern sowie die Handwerkskammern sind gute Ansprechpartner.

5 Security Maßnahmen

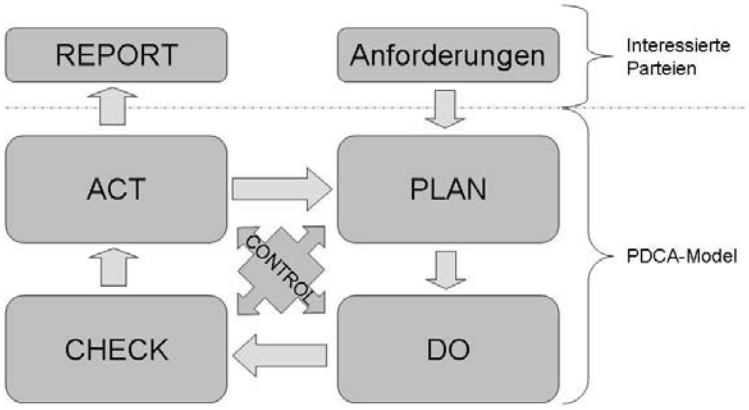


Abbildung 27: Security Maßnahmen

Nachdem im Kapitel 2 das Security Management als Prozess vorgestellt worden ist, und im Kapitel 3 die Schnittstellen des Security Management mit den anderen ITIL Prozessen untersucht worden ist, werden in diesem Kapitel die Maßnahmen beschrieben, die ergriffen werden müssen, um die Sicherheitsziele zu erreichen.

Analog zu ITIL werden hier die Maßnahmen aus der ISO/IEC 17799 in der aktuellsten Fassung von 2005 als Basis genommen. Um eine Wiedererkennung zu erleichtern, wird hier jeweils die Nummerierung aus dem Code of Practice übernommen, wie er sich auch im Annex A des ISO/IEC 27001:2005 wiederfindet. Der Aufbau der Abschnitte folgt ebenfalls dem Code of Practice, indem er das Ziel der Maßnahmengruppe definiert und darunter die wichtigsten Maßnahmen auflistet.

Wie in Kapitel 4 beschrieben, können auch andere Maßnahmenkataloge, wie zum Beispiel der Maßnahmenkatalog aus dem BSI Grundschutzhandbuch genommen werden. ITIL schreibt hier keinen bestimmten Katalog vor.

In den folgenden Abschnitten soll beispielhaft die Methode verdeutlicht werden, mit der aus einem Maßnahmenkatalog die Zuteilung in die Phasen des Security Managements Prozesses vorgenommen werden kann.

Lediglich die Report-Phase, die bereits ausführlich beschrieben worden ist, wird nicht weiter untersucht.

5.1 Anforderungen

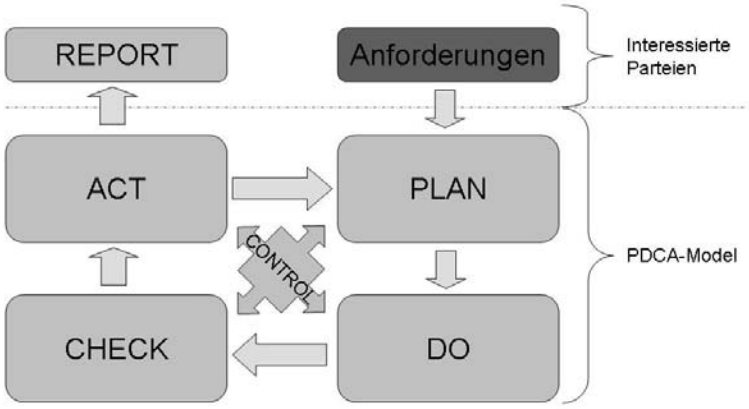


Abbildung 28: Security Maßnahmen – Anforderungen

[12] Anschaffung, Entwicklung und Wartung von IT-Services

[12.1.] Sicherheitsanforderungen an IT-Services

Ziel:

Ziel ist es, dass die IS ein integraler Bestandteil der IT-Services ist. Im Hinblick auf die Entwicklung wird in diesem Zusammenhang häufig von „Designed for Security“ gesprochen.

Maßnahmen:

- Am meisten kann für die IS getan werden, wenn diese bereits bei der Planung von neuen IT-Services berücksichtigt werden, und die somit definierten Sicherheitsziele konsequent umgesetzt werden.
- Dazu müssen für jede identifizierte Anforderung Testfälle erzeugt werden, die als Abnahmekriterium gelten.

Da ITIL keinen Fokus auf die Software-Entwicklung legt, ist es hier Aufgabe des Security Managers die Projekte bezüglich der richtigen Auswahl von Qualitätskriterien und Testkriterien zu unterstützen.

[15] Compliance

Ziel:

Compliance hat die Identifikation aller Anforderungen zum Ziel, um diese einzuhalten.

Maßnahmen:

- Identifikation von gesetzlichen Anforderungen
- Identifikation von Anforderungen an das DRM
- Identifikation der organisatorischen Anforderungen.

Diese Anforderungen werden innerhalb von ITIL durch das Service Level Management gesammelt und zu SLAs verdichtet. Das Security Management hilft durch das Wissen und die adäquate Methodik, die geeigneten Anforderungen zu identifizieren und die Sicherheitsziele der SLAs zu definieren.

5.2 Control

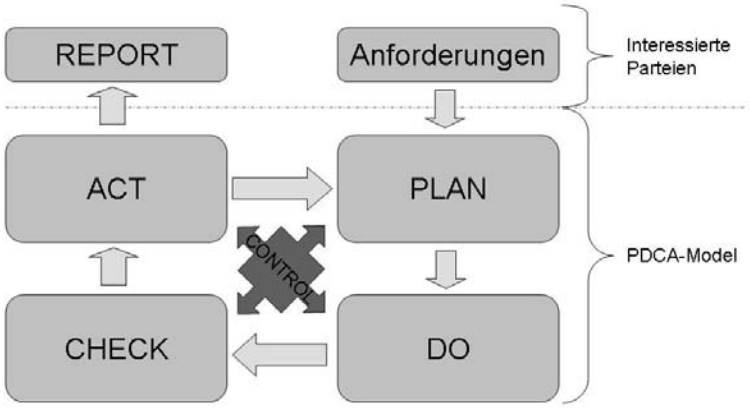


Abbildung 29: Security Maßnahmen – Control

Während der Control-Phase wird die Organisation des Security Management Prozesses definiert.

In dem Standard ISO/IEC 27001:2005 wird definiert, was getan werden muss, um ein ISMS zu definieren, zu implementieren und zu betreiben. Diese Anforderungen an ein ISMS werden durch die Maßnahmen, die im Annex A und im Code if Practice beschrieben sind, konkretisiert.

[6] Organisation der IS

[6.1.] Interne Organisation

Ziel:

Sämtliche Aufgaben der IS müssen innerhalb des Unternehmens verwaltet werden. Dazu muss eine Struktur aufgebaut werden, nach der diese geplant, implementiert, überwacht und gepflegt werden können.

Maßnahmen:

- Die Unternehmensleitung sollte eine aktive Rolle im Security Management Prozess spielen unddiese durch übergeordnete Vorgaben steuern. Dazu gehört, dass durch die Unternehmensleitung die Verantwortlichkeiten eindeutig festgelegt, und diese aktiv kommuniziert werden
- Die Aufgaben, die es innerhalb des Security Management Prozesses gibt, müssen aufgeteilt werden, wobei auf die Trennung der Funktionen geachtet werden muss
- Jedes CI muss einem Verantwortlichen zugeordnet werden
- Abnahme- und Freigabeverfahren für neue oder geänderte IT-Services und Maßnahmen müssen geregelt werden
- Es muss definiert werden, welche Rollen es innerhalb des Security Managements gibt und welche Anforderungen an Verschwiegenheit und Geheimhaltung bestehen
- Die Schnittstelle zu anderen Prozessen muss festgelegt werden
- Es sollte ein regelmäßiges Treffen eingerichtet werden, an dem allen relevanten Beteiligten teilnehmen sollten, zum Beispiel Unternehmensleitung, Security Manager, IT-Leitung, mittlere Führungsebene, etc. Auf diesem Treffen sollten aktuelle Fragestellungen der IS, Entwicklungen, Trends sowie anstehende Änderungen besprochen werden. Ebenfalls sollten hier regelmäßig Bewertungen vorgenommen werden, wie effektiv und effizient die Sicherheitsziele erreicht worden sind

- Bei der Verbindung zu weiteren beteiligten Gruppen und dem Staat muss festgelegt werden, wer Anforderungen von diesen aufnehmen darf und welche Informationen diesen gegeben werden dürfen
- Eine regelmäßige Überprüfung der internen Organisation muss festgelegt werden.

[6.2.] Organisation externer Beteiligter

Ziel:

Das Ziel ist die Organisation der IS für jegliche Nutzung von IT-Services oder Zugriffe zu Informationen durch Externe. Externe können dabei zum Beispiel Wartungsmitarbeiter und Berater sein, die innerhalb des eigenen Netzwerkes arbeiten, aber auch Kunden, die IT-Services nutzen.

Maßnahmen:

- Das Risiko, das entsteht, wenn Externe auf IT-Services oder Informationen zugreifen, muss identifiziert und analysiert werden
- Es muss eine risikobasierte Auswahl von Maßnahmen erfolgen
- Die identifizierten Anforderungen an die IS und die daraus abgeleiteten Maßnahmen müssen den Externen kommuniziert werden.
    - Bei Kundenbeziehungen wird dieses innerhalb des SLA in der Security Section beschrieben
    - Bei Lieferanten- oder Kooperationspartnern werden diese Anforderungen in gegenseitigen Verträgen und Vereinbarungen definiert.

5.3 Plan

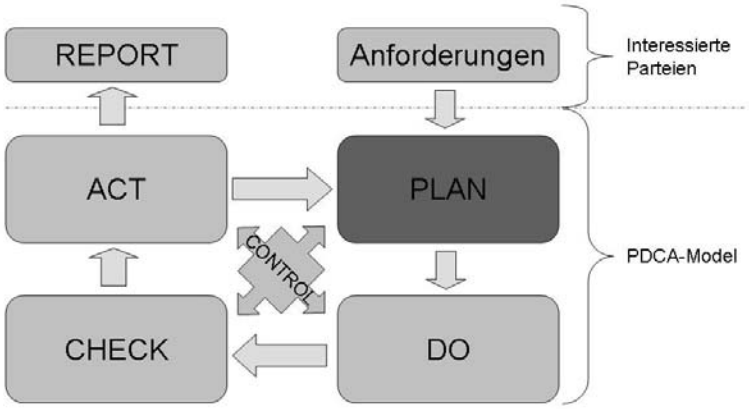


Abbildung 30: Security Maßnahmen - Plan

[5] Security Policy

[5.1.] Information Security Policy

Ziel:

Eine IS-Policy hat das Ziel, die Ausrichtung der Unternehmensleitung auf die IS und deren Unterstützung zu manifestieren.

Maßnahmen:

- Erstellung einer Policy
- Definition der übergeordneten Sicherheitsziele, zum Beispiel die Unterstützung der Geschäftsprozesse durch sichere IT-Services
- Definition von Umfang und Abgrenzung
- Definition einer Rahmenstruktur, die festlegt, wie Maßnahmen beschrieben werden müssen
- Definition einer Rahmenstruktur für das Berichtswesen

- Definition der Verantwortlichkeiten innerhalb des Security Management Prozesses
- Festlegung einer Risiko Management Methode
- Referenz zu mitgeltenden Dokumenten.

5.4 Do

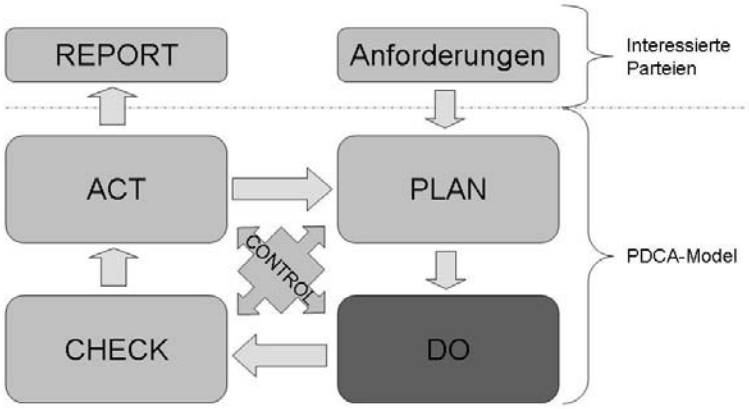


Abbildung 31: Security Maßnahmen - Do

[7] Verwaltung der Assets

[7.1.] Verantwortlichkeit für Assets

Ziel:

Für jedes CI muss ein Eigner identifiziert werden, der dafür verantwortlich ist, dass geeignete Maßnahmen ausgewählt worden sind und diese einwandfrei funktionieren. Ein Eigner kann die Aufgabe der Implementierung von Maßnahmen an einen Dritten delegieren, er behält jedoch die Verantwortung.

Maßnahmen:

- Alle CI müssen identifiziert, dokumentiert und gepflegt werden. Bei ITIL werden alle Assets durch das Configuration Management verwaltet. Diese verantwortet die CMDB, in der alle CIs aufgelistet sind
- Alle Änderungen an den CIs müssen identifiziert, genehmigt und dokumentiert werden. Diese Aufgabe übernimmt bei ITIL das Change Management
- Jedes CI muss einen eindeutigen Eigner haben, der
  - die Klassifizierung der CIs hinsichtlich der IS Qualitätsmerkmale vornimmt und
  - den Zugriff auf das CI definiert und regelmäßig überprüft.
- Für alle CIs muss festgelegt sein, wofür diese benutzt werden dürfen und wofür eine Benutzung ausgeschlossen ist
- Beispielsweise muss festgelegt sein, wofür ein Notebook eines Aussendienstmitarbeiters genutzt werden darfund ob neben der geschäftlichen Nutzung der E-Mail auch die private gestattet ist.

[7.2.] Klassifizierung von Informationen

Ziel:

Die IS Anforderungen an Informationen müssen definiert werden, damit ein angemessenes und wirtschaftliches Maß von Schutzmaßnahmen ausgewählt werden kann.

Maßnahmen:

- Um für Informationen angemessene Schutzmaßnahmen festzulegen, müssen die Anforderungen an die Merkmale der IS definiert sein. Dieses sind beispielsweise Vertraulichkeit, Integrität und verfügbarkeit.
- Es muss ein Verfahren festgelegt werden, wie Klassifikationen durchzuführen sind, und nach welchen Kriterien diese zu erfolgen haben

- Sinnvolle Bezeichnungen müssen sowohl für physische CIs, wie auch für elektronischen CIs gefunden werden
- Beispielsweise ist eine einheitliche Datenträgerbeschriftung sinnvoll sowie eine einheitliche Dateiablage, unter der eine feste Nomenklatur eingehalten wird.

[8] IS bei Beschäftigten

[8.1.] Vor Beschäftigungsbeginn

Ziel:

Es muss sichergestellt werden, dass Angestellte und Fremdarbeiter ihre Pflichten in Bezug auf die sichere Nutzung der IT verstehen. Weiterhin muss die Befähigung dieser Anwender sichergestellt werden sowie das Risiko von Diebstahl, Betrug und Zerstörung minimiert werden. Dieses muss jeweils zu Beginn und bei Änderung der zugewiesenen Rolle geschehen.

Maßnahmen:

- Die Rollen und Verantwortlichkeiten aller Anwender an die IT-Services müssen definiert werden
- Jeder Anwender muss die Sicherheitsziele kennen und aktiv unterstützen
- Jeder Anwender muss die ihm zugewiesenen CIs vor Diebstahl, Offenlegung, Veränderung und Zerstörung schützen
- Jeder Anwender muss eventuell IS-Maßnahmen selber ausführen, zum Beispiel den manuellen Start eines Anti-MalWare Programms
- Jeder Anwender trägt die volle Verantwortung für sein Handeln.
- Jeder Anwender muss Security Incidents umgehend melden und die Aufklärung erleichtern, indem er zum Beispiel Screenshots von Warnmeldungen macht

- Um die Befähigung und persönliche Integrität eines Bewerbers bewerten zu können, müssen je nach Grad der Sicherheitsanforderungen Untersuchungen und Prüfungen vorgenommen werden, die zum Beispiel seine Fachkunde verdeutlichen, sein Sozialverhalten beleuchten und seine berufliche Vergangenheit hinterfragen. Bei hochsensiblen Bereichen können staatliche Nachweise wie zum Beispiel ein Führungszeugnis gefordert werden
- Jede Vereinbarung mit einem Anwender muss schriftlich festgehalten und diesem ausreichend erläutert sowie von ihm abgezeichnet werden.

[8.2.] Während der Beschäftigung

Ziel:

Es muss sichergestellt werden, dass Anwender - sowohl Angestellte wie auch Fremdarbeiter - die Bedrohungen kennen, die für CIs bestehen, die durch sie genutzt werden. Weiterhin müssen sie ihre Pflichten in Bezug auf die sichere Nutzung der IT kennen und es muss sichergestellt werden, dass alle Anwender angemessen ausgebildet sind und die nötigen Verfahren und Maßnahmen beherrschen, die sie zum Erreichen der Sicherheitsziele benötigen.

Maßnahmen:

- Jeder Vorgesetzte trägt dafür Sorge, dass seine Mitarbeiter in Bezug auf die Sicherheitsziele informiert sind und die Erreichung der Sicherheitsziele soweit wie möglich überprüft wird. Das kann zum Beispiel eine Überprüfung sein, ob ein Mitarbeiter alle Dokumente nach der richtigen Nomenklatur benannt hat oder seinen Arbeitsplatz-PC sperrt, wenn er nicht in seinem Büro ist

- Ein wichtiger Baustein ist das Training von Anwendern in Bezug auf Bedrohungen und Maßnahmen. Solche Trainings werden häufig zu Awareness Kampagnen zusammengefasst, die neben der funktionalen Vermittlung des Themas IS auch die organisatorische Ebene ansprechen, also wie ein Security Incident gemeldet werden muss und wer der richtige Ansprechpartner ist. Solche Awareness Kampagnen können ganz unterschiedliche Formate haben, vom unternehmensweiten Aktionstag über Computer Based Trainings (CBT) bis zum Event auf der Theaterbühne mit Quiz und anschließenden Sektempfang
- Ebenfalls wichtig ist die Schulung der benutzten IT-Services. Hier sollte in die allgemeinen Schulungen, beispielsweise für die richtige Benutzung einer Software-Anwendung, immer eine IS-Komponente eingebaut werden
- Wenn Verstöße gegen bestehende Maßnahmen auftreten, müssen diese sanktioniert werden. Diese disziplinarischen Regelungen müssen verbindlich und für alle verständlich festgelegt und dokumentiert werden, ähnlich einem Bußgeldkatalog.

[8.3.] Bei Beendigung oder Änderung des Beschäftigungsverhältnisses

Ziel:

Es muss sichergestellt werden, dass Angestellte und Fremdarbeiter, die eine Beschäftigung beenden, alle Unterlagen, sowohl physische, wie auch elektronische und die Ausrüstungsgegenstände, zum Beispiel Handy und Notebook, sowie Zutrittskarten abgeben. Weiterhin muss sichergestellt werden, dass Geheimhaltungsverpflichtungen auch über die Beendigung der Beschäftigung hinaus eingehalten werden. Jede Änderung eines Beschäftigtenverhältnisses sollte wie eine Beendigung behandelt werden. Für die Aufnahme der neuen Beschäftigung gelten die Maßnahmen analog zu [8.1.]

Maßnahmen:

- Es muss festgelegt werden, welche Sicherheitsziele und welche Geheimhaltungsverpflichtung weiterhin für den Anwender gelten

- Es müssen alle persönlich genutzten Ausrüstungsgegenstände zurückgegeben werden, wie zum Beispiel

  - Handy
  - Notebook
  - Backup-Medien
  - Sonstige Medien mit Daten des Unternehmens
  - Bücher
  - Schulungsunterlagen
  - Telework Ausrüstung (Drucker, Router, PC)

- Ebenso müssen alle Kennworte übergeben werden, die ein Anwender im Namen des Unternehmens bei Dritten hatte, zum Beispiel

  - Zugangskennung zum Intranet eines Kooperationspartners
  - Zugang zu kostenpflichtigen oder lizenzierten Webseiten und Recherchediensten
  - Zugangskennung für ein privat genutztes E-Mail Konto, welches das Unternehmen als Leistung für die Mitarbeiter bezahlt

- Bei den Zugangsdaten für Dritte muss das Passwort des ausscheidenden Anwenders umgehend geändert werden
- Auf sämtlichen Systemen, in sämtlichen Datenbanken und allen Software-Anwendungen müssen die Rechte widerrufen und der Anwender gesperrt werden.

[9] Physische Sicherheit

ITIL betrachtet die physische Sicherheit nicht. Da diese jedoch wichtig für die Erreichung der Sicherheitsziele ist, wird diese hier aufgeführt.

[9.1.] Abgesicherte Arbeitsbereiche

Ziele:

Es ist das Ziel, Unbefugten den Zutritt zu verwehren beziehungsweise diese schnell identifizieren zu können.

Maßnahmen:

- Errichtung von Zäunen, Schranken und Toren
- Außenüberwachung von unübersichtlichen und kritischen Stellen durch Kameras
- Einrichtung eines Empfangstresens, der durch Sicherheitskräfte besetzt ist
- Identifikation aller Mitarbeiter, Lieferanten, Besucher und externer Mitarbeiter. Beispielsweise geben einige Unternehmen verschiedenfarbige Schlüsselbänder mit dem Besucherausweis an die Besucher, mit dem Hinweis, dass diese Besucherausweise offen getragen werden müssen. Dabei steht jede Farbe für einen bestimmten Grad an Vertrauenswürdigkeit. Sollte jetzt ein Besucher mit einem Besucherausweis allein auf dem Flur angetroffen werden, der ein niedriges Maß an Vertrauenswürdigkeit hat, handelte sich offensichtlich um einen Security Incident
- Alle Büroräume sollten abschließbar sein beziehungsweise sollten in großen und Großraumbüros abschließbare Schränke für Mitarbeiter vorhanden sein
- Die notwendigen Präventionsmaßnahmen gegen Feuer, Wasser, Blitzschlag, etc. müssen getroffen werden.

[9.2.] Gerätesicherheit

Ziel:

Schutz aller CIs vor Beschädigung, Diebstahl und Kompromittierung.

Maßnahmen:

- Systeme müssen in sicheren und speziell ausgerüsteten Räumen aufgestellt werden, zum Beispiel Server in Serverräumen oder Rechenzentren, und Netzwerkkomponenten in Netzwerkschränken. Diese Räume und Schränke müssen ausreichend gesichert sein
- Die Gefahr einer Stromunterbrechung muss durch geeignete Maßnahmen, zum Beispiel eine unterbrechungsfreie Stromversorgung gemindert werden. Bei diesen Maßnahmen muss durch einen Wartungsplan die Funktionsfähigkeit überprüft werden
- Alle Kabel müssen sicher verlegt sein
- Aussortierte Systeme müssen sicher entsorgt werden, so dass keine Informationen aus dem Unternehmen heraus gelangen können, die beispielsweise noch auf der Festplatte gespeichert sind
- Es müssen Verfahren entwickelt und implementiert werden, wie Geräte, die außerhalb des Unternehmens genutzt werden, gesichert werden können.

[10] Kommunikation und IT-Betrieb

[10.1.] IT-Betrieb und Verantwortlichkeiten

Ziel:

Schutz der IT-Produktion

Maßnahmen:

- Für alle IT-Betriebsprozesse und Maßnahmen, welche die Sicherheitsziele betreffen, muss eine aktuelle Dokumentation vorliegen, die gemäß den Dokumentationsvorschriften in der IS-Policy verfasst ist
- Es muss ein Verfahren implementiert sein, das alle Änderungen an der IT erfasst, bewertet und autorisiert. Dieses wird bei ITIL durch das Change Management sichergestellt

- Es muss eine Trennung von Verantwortlichkeiten und Funktionen geben, so dass nicht Planungs-, Implementierungs- und Prüfungsaufgaben durch einen Mitarbeiter ausgeführt werden
- Die Entwicklungs-, Test- und Produktionssysteme müssen voneinander getrennt sein, so dass keine negativen Auswirkungen durch Änderungen an Entwicklungssystemen, oder beispielsweise durch Lasttests in der Testumgebung auf die Produktionsumgebung entstehen. Weiterhin muss dafür gesorgt werden, dass die Produktions- und die Testsysteme gleichartig sind, so dass Aussagen zur Lauffähigkeit einer Software-Anwendung, die auf einem Testsystem getroffen worden sind, auch auf dem Produktionssystem Gültigkeit haben.

[10.2.] Service Delivery Management für Dritte

Ziel:

Es muss sichergestellt werde, dass Sicherheitsziele, die in der Security Section eines SLA definiert worden sind, eingehalten werden können.

Maßnahmen:

- Vereinbarung von Sicherheitszielen und Definition von Kennzahlen, welche die Erreichung der Ziele messen können. Dieses wird bei ITIL durch das Service Level Management sowie weitere Prozesse aus dem Service Delivery sichergestellt
- Die erbrachten IT-Services sollten in Bezug auf Security Incidents regelmäßig überprüft sowie permanent überwacht werden
- Es muss ein geeignetes Verfahren festgelegt werden, um Änderungen für die Erbringung von Services zu erfassen, zu bewerten und autorisieren. Dieses wird bei ITIL durch das Change Management sichergestellt.

[10.3.] Systemplanung und Abnahme

Ziele:

Die Minimierung des Risikos, dass nach Änderungen oder Neueinführungen Störung auf dem Produktionssystem auftreten.

Maßnahmen:

- Die Benutzung von IT-Ressourcen muss geplant, überwacht und optimiert werden, um die geforderte Leistungsfähigkeit der IT-Services sicherzustellen. Diese Aufgabe wird bei ITIL durch das Capacity Management sichergestellt
- Zur verbindlichen Abnahme eines neuen Systems müssen im Vorfeld Kriterien entwickelt werden, die als Abnahmenmaßstab gelten. Dieses sind zum Beispiel Testfälle für funktionale Prüfungen oder Testszenarien, in denen beispielsweise das Lastverhalten oder die Fehlertoleranz von Systemen getestet wird
- Wichtig ist, dass die Kriterien zur Abnahme auf Basis der Anforderungen, beispielsweise des Fachkonzeptes einer Software-Anwendung, entwickelt werden. Ebenfalls ist es ratsam, die Test- und Abnahmekriterien auf Basis einer Risikobewertung vorzunehmen, um die risikoreichen Funktionen vernünftig abzudecken.

[10.4.] Schutz gegen MalWare und Mobile Code

Ziele:

Schutz der Integrität

Maßnahmen:

- Es muss ein angemessener Schutz gegen MalWare implementiert sein
- Erkennung von MalWare muss sichergestellt sein. Auf Basis einer Risikobewertung muss festgelegt werden, wie hoch der Schutzbedarf für die IT-Services und Informationen ist, und gemäß dieser Bewertung müssen Maßnahmen ausgewählt werden

- Durch die Verwendung mehrerer Anti-MalWare Programme an unterschiedlichen Stellen innerhalb der IT-Infrastruktur wird ein so genanntes Cross-Checking ermöglicht, in dem MalWare an verschiedenen Stellen erkannt werden kann. Hierdurch wird der Problematik durch nicht aktuelle Anti-MalWare Programme vorgebeugt. Durch eine immer schnellere Verbreitung von MalWare ist Aktualisierung häufig im Stundentakt notwendig, um IT-Services und Informationen vor MalWare zu schützen
- Die Verhinderung von dem Ausbreiten über mehrere Netzwerke oder Arbeitsplatz-PCs und Server ist notwendig, da jeder Infektionspunkt eine Vervielfachung der Ansteckungsgefahr der Systeme mit sich bringt
- Eine saubere Entfernung von MalWare ist notwendig, gestaltet sich in der Realität aber häufig als schwierig, da durch den enormen Anstieg der MalWare eine saubere Definition des Schadens kaum noch vorgenommen werden kann. Die Anti-MalWare Labore müssen großen Aufwand betreiben, in kürzester Zeit eine akkurate Erkennung von neuer MalWare zu gewährleisten, so dass viele Anti-MalWare Produkte kein sauberes Entfernen mehr beherrschen
- Die Wiederherstellung eines Systems muss sichergestellt sein, beispielsweise durch die Wiederherstellung einer Sicherungskopie
- Bei den Anwendern muss Achtsamkeit (Awareness) gegenüber den Auswirkungen von achtlos geöffneten E-Mail-Anhängen und Internetseiten erzeugt werden. Hier müssen die Bedrohungen und die Verfahren für ein sicheres Arbeiten mit dem Arbeitsplatz-PC regelmäßig vermittelt werden
- Es muss ein angemessener Schutz gegen Mobile Code implementiert sein
- Es darf nur genehmigter Code ausgeführt werden. Dieser muss als solcher gekennzeichnet sein, zum Beispiel durch geeignete Zertifikate
- Nicht genehmigter Code darf nicht zur Ausführung gelangen und sollte nicht im Netzwerk verfügbar sein.

[10.5.] Informationssicherung (Backup)

Ziel:

Die Integrität und die Verfügbarkeit von Informationen und IT-Services müssen sichergestellt sein.

Maßnahmen:

- Die Anforderungen an Informationssicherung müssen festgelegt werden
- Es müssen von allen Informationen in regelmäßigen Abständen Sicherungskopien erstellt werden
- Die Sicherungskopien sollten regelmäßig auf ihre korrekte Speicherung und den Inhalt hin untersucht werden
- Wiederherstelltests müssen regelmäßig durchgeführt werden
- Sicherungskopien sollten gemäß ihren Anforderungen an einem sicheren Ort aufbewahrt werden, der nicht in unmittelbarer Nähe zu dem Informationssystem sein darf, von dem die Sicherungskopie erstellt worden ist
- Wo nötig sollten Sicherungskopien ausgelagert werden. Hierbei ist zu beachten, dass die Sicherungskopien gegen Veränderung und gegen unbefugten Zugriff zu sichern sind
- Bei hohem Schutzbedarf und sehr geringer Wiederherstellzeit sollte eine online Sicherungskopie erstellt werden, beispielsweise in eine virtuelle Sicherungsbibliothek (Virtual Tape Library, VTL).

[10.6.] Schutz des Netzwerkes

Ziel:

Schutz sämtlicher Informationen, die in dem Unternehmensnetzwerk transportiert werden, ebenso wie die Informationen, die in das Netzwerk hineinkommen und aus dem Netzwerk hinausgehen.

Maßnahmen:

- Netze sollte so betrieben werden, dass Bedrohungen nicht in ein Netzwerk hineingelangen und dort CIs angreifen können
- Ebenfalls muss verhindert werden, dass klassifizierte Informationen aus dem Netzwerk unbefugt nach außen
- Eine Bedrohung, die aus dem Netzwerk heraus andere Netzwerke bedroht, muss verhindert werden
- Die Anforderungen an die Sicherheitsziele für Netzwerke müssen in der Security Section in den SLA festgelegt werden. Diese Aufgabe wird bei ITIL durch das Service Level Management sichergestellt.

[10.7.] Handhabung von Medien und Datenträgern

Ziel:

Medien und Datenträger sollten überwacht und physisch gesichert sein, um unbefugte Nutzung, Veränderung, Entfernung oder Zerstörung zu verhindern.

Maßnahmen:

- Es muss ein Verfahren implementiert sein, das die Verwaltung von Datenträgern sicherstellt
- Die sichere Aufbewahrung von Datenträgern muss gewährleistet sein
- Registrierung von Datenträger und Einhaltung der Namenskonventionen
- Datenträger sollten nur dann benutzt werden, wenn es eine geschäftliche Anforderung gibt
- Die Entsorgung alter und nicht mehr genutzter Datenträger muss gemäß den Anforderungen an Vertraulichkeit sichergestellt werden. Dazu kann ein geeignetes Lösch- oder Formatierungsverfahren ausgewählt werden sowie eine Datenträgertonne, die verschlossen ist und durch ein zertifiziertes Entsorgungsunternehmen abgeholt und geleert wird

- Für den Umgang mit Medien muss ein Verfahren implementiert sein, dass die Benutzung von Medien und die Beschriftung regelt, die Zugangs- und Zugriffsrechte verwaltet und die Speicherung überwacht
- Alle Kopien von Datenträgern und Medien sind als Kopien zu kennzeichnen
- Systemdokumente sollten generell gegen unbefugten Zugriff geschützt sein.

[10.8.] Informationsaustausch

Ziel:

Die Sicherheitsziele müssen beim Austausch von Informationen innerhalb von Unternehmen und über Unternehmensgrenzen hinweg sichergestellt sein.

Maßnahmen:

- Die Vertraulichkeit muss bei der Übertragung durch geeignete Maßnahmen geschützt sein, zum Beispiel durch Kryptographie
- Ebenso muss der Schutz der Integrität gewährleistet werden können, beispielsweise durch Anti-MalWare Programme
- Bei drahtlosen Netzwerkverbindungen sollten geeignete Verfahren zu Einsatz kommen, die sicherstellen, dass keine ungewollten und nicht autorisierten Verbindungen zustande kommen, und gleichzeitig die Vertraulichkeit der Information gewährleisten, die über die Netzwerke ausgetauscht wird
- Es müssen Richtlinien implementiert sein, die festlegen, welche Art von Informationen auf welche Weise ausgetauscht werden müssen. Beispielsweise sollten hochsensible Informationen nicht per E-Mail geschickt werden. Hier sollte auch festgelegt sein, dass niemals auf E-Mails geantwortet werden darf, die von unbekannten Versendern mit nicht plausiblem Text kommen
- Nationale Richtlinien müssen ebenso berücksichtigt werden wie internationale

- Für die Kommunikation zwischen Unternehmen und in Projekten sollten verbindlichen Vereinbarungen getroffen werden

  - auf welche Art Informationen ausgetauscht werden müssen,
  - welche Formate dazu benutzt werden sollen,
  - welche Namenskonventionen gelten,
  - welche Sicherheitsziele definiert werden,
  - welche IS-Maßnahmen angewandt werden müssen, zum Beispiel Kryptografie,
  - welche Pflichten Absender und Empfänger haben und
  - wann ein Austausch verbindlich ist.

- Datenträger, die das Unternehmen verlassen, müssen gemäß den enthaltenen und klassifizierten Informationen geschützt werden
- Elektronische Nachrichten, wie zum Beispiel EDI, E-Mail oder Instant Messaging müssen angemessen geschützt werden.

[10.9.] Elektronische Handelssysteme (E-Commerce)

Ziele:

Ziel ist es, die Informationen zu schützen, die durch E-Commerce einer Öffentlichkeit verfügbar gemacht werden, sowie die zu diesem Zweck genutzten Systeme.

Maßnahmen:

- Internet-Anwendungen stellen besondere Herausforderungen an die IS da, da häufig Informationen über zahlreiche Netzwerke und Systeme transportiert werden
- Die Sicherheitsziele müssen definiert werden, ebenso müssen die Qualitätsmerkmale ausgewählt werden

- Die Informationen müssen klassifiziert werden, damit angemessene Maßnahmen, wie zum Beispiel Verschlüsselung oder Zwei-Faktor Authentifikation, die Einhaltung der Sicherheitsziele sicherstellen können
- Es sollte eine Protokollierung durchgeführt werden, die aussagekräftig ist, wenn es um Nachvollziehbarkeit von Transaktionen und Security Incidents geht
- Kunden und Geschäftspartner müssen über die Maßnahmen und Protokollierungen informiert werden
- Sofern Bezahlmöglichkeit implementiert sind, müssen diese hinsichtlich Schutz und Nachvollziehbarkeit untersucht und entsprechend geschützt werden.

[10.10.] Überwachung (Monitoring) und Protokollierung

Ziel:

Security Incidents müssen identifiziert werden.

Maßnahmen:

- IT-Ereignisse, wie zum Beispiel das Anmelden an ein System und Fehlermeldungen, sollten protokolliert werden. Dazu müssen die geeigneten Daten ausgewählt werden, wie auch der Zeitpunkt der Protokollierung
- Protokolldateien müssen sicher abgespeichert werden und vor Veränderung und Löschung geschützt sein
- Protokolldateien sollten für eine bestimmte Zeit aufbewahrt werden, damit diese auch später noch für Analysezwecke genutzt werden können
- Die Aktivität von Administratoren und Anwendern mit besonderen Rechten sollte gesondert protokolliert werden
- Für die Protokollierung müssen Zeitstempel gesetzt werden
- Es sollten Verfahren implementiert werden, welche die Systemnutzung überwachen. Die Ergebnisse müssen regelmäßig überprüft werden
- Eine Risikobewertung sollte dem Umfang und der Intensität der Verfahren zugrunde liegen.

[11] Zugriffskontrolle

Ziel:

Die Zugriffe auf Informationen müssen kontrolliert werden.

Maßnahmen:

- Es muss eine Zugriffskontroll-Policy definiert werden, in der unter anderem festgelegt wird

  - auf welche Art Zugriffe beantragt werden können
  - welche standardisierten Anwenderrollen inklusive der Zugriffsrechte es gibt und
  - wie Zugriffsrechte entzogen werden können.

[11.2.] Zugriffsrechte für Anwender

Ziel:

Autorisierte Anwender benötigen Zugriffsrechte auf Informationen und IT-Services. Nicht autorisierte Anwender und unbefugte Dritte dürfen keinen Zugriff zu Informationen und IT-Services erlangen.

Maßnahmen:

- Anwender müssen durch eine eindeutige Identifikation (ID) in einer Anwenderdatei registriert werden
- Es muss eine formale Autorisierung durch den Eigner der Systeme und den Vorgesetzten erfolgen
- Die Anwender müssen über die Pflichten und Protokollierungen sowie IS-Maßnahmen informiert werden
- Zugriffsrechte müssen beim Ausscheiden, bei der Änderungen der Rolle sowie bei längeren Abwesenheitszeiten (Elternschutz, lange Krankheit, Sabatical) widerrufen werden
- Für die Rechtevergabe gilt der Grundsatz „Need to know“, das heißt, ein Anwender muss so viele Rechte wie nötig und so wenige wie möglich erhalten

- Wo die Geschäftsprozesse dieses fordern, können auch zeitlich begrenzte Zugriffsrechte erteilt werden
- Zur sicheren Authentifikation benötigt jeder Anwender ein Passwort, das er selbst erzeugt und regelmäßig ändern muss
- Zur Erstellung und dem Gebrauch von Passwörtern muss eine Policy erstellt werden, die ebenfalls regelt, wann ein Passwort als sicher angesehen werden kann
- In der Policy sollte weiterhin definiert sein, dass Standardkennungen und Passwörter, die in Systemen und Software-Anwendungen voreingestellt sind, sofort zu ändern sind
- Persönliche Passwörter dürfen nicht weitergegeben werden und Gruppenpasswörter sollten vermieden werden. Wenn eine Führungskraft entscheidet, dass in seinem Bereich Gruppenpasswörter Anwendung finden sollen, ist diese Entscheidung aufzunehmen
- Passwörter sollten nicht auf Systemen gespeichert werden, wie zum Beispiel im Browser für Internetzugänge oder bei Systemanmeldungen.

[11.3.] Verpflichtung der Anwender

Ziel:

Anwender müssen über ihre Pflichten informiert werden, da die Kooperation zwischen Security Management und Anwender für die Erreichung der Sicherheitsziele unumgänglich ist.

Maßnahmen:

- Jeder Anwender muss auf Einhaltung der Passwort-Policy verpflichtet werden
- Sobald ein Anwender seinen Arbeitsplatz verlässt, muss er sich aus dem System abmelden (Logoff) sowie bearbeitete Dateien speichern und aktive Verbindungen schließen. Dies ist die so genannte Clear Screen Policy
- Falls ein Anwender ein Notebook verwendet, muss er durch geeignete Maßnahmen dafür sorgen, dass dieses nicht entwendet werden kann, zum Beispiel indem er es einschließt oder durch die Benutzung eines Notebook-Schlosses

- Ebenfalls muss ein Anwender sämtliche Datenträger, Kleingeräte (wie Handy und PDA) sowie Ausdrucke mit vertraulichem Inhalt von seinem Arbeitsplatz entfernen, wenn er den Arbeitsplatz verlässt. Dieses nennt man Clear Desk Policy
- Ausdrucke, die ein Anwender veranlasst, muss dieser umgehend aus dem Drucker entnehmen. Für sensible Bereiche können Drucker auch mit Passwort oder PIN zugreifbar gemacht werden, so dass die Ausdrucke erst dann ausgegeben werden, wenn der Anwender am Drucker steht.

[11.4.] Zugriffskontrolle Netzwerk

Ziel:

Schutz vor unbefugten Zugriffen auf Netzwerke und Netzwerkservices.

Maßnahmen:

- Es sind angemessene Schnittstellen zwischen dem Netzwerk eines Unternehmens, den Netzwerken weiterer Unternehmen und öffentlichen Netzwerken implementiert, beispielsweise durch Firewalls
- Entsprechende Verfahren zur Authentifikation von Anwendern müssen etabliert sein
- Eine Überwachung von Anwenderzugriffen innerhalb eines Netzwerkes auf Informationen, IT-Services und Netzwerkdienste muss stattfinden
- Es muss eine Policy zur Benutzung von Netzwerken und Netzwerkdiensten definiert worden sein, die festlegt, welche Netzwerke und Netzwerkdienste zugelassen sind und die geeignete Authentifikationsverfahren beschreibt
- Die Authentifikationsverfahren für externe Verbindungen müssen angemessen sein bezüglich der Risikobewertung der genutzten Informationen und CIs. Hier sollte darauf geachtet werden, dass es ein standardisiertes Verfahren zur Authentifikation gibt
- Die Systeme sollten im Netzwerk eindeutig identifizierbar und lokalisierbar sein

- Fernwartungs- und Konfigurationszugänge sollten nur dann genutzt werden, wenn diese nicht benötigt werden. Wenn sie gebraucht werden, sollten sie temporär angeschaltet und überwacht sowie protokolliert werden
- Bestimmte Anwendergruppen, sowie die Datenbanken und Systeme sollten sich in getrennten Netzwerksegmenten befinden. Die Trennung der Netzwerke kann durch logische Trennung, physikalische Trennung, Trennung durch Firewalls oder Verschlüsselungstechnik (VPN) erfolgen
- Die Netzwerke und Netzwerkdienste sollten gemäß den Anforderungen der Informationen und IT-Services abgesichert sein
- Die Nutzung von Netzwerken und Netzwerkdiensten sollte nur aufgrund geschäftlicher Anforderungen geschehen. Daher muss überwacht werden, welche Verbindungen durch Anwender genutzt werden und möglicherweise, zu welchem Zweck dies geschieht. Üblicherweise wird dieses an den Schnittstellen zu anderen Netzwerken, zum Beispiel dem Internet, gemacht. Beispielsweise wird einem Anwender der Versand und Empfang von E-Mails ausschließlich über den unternehmensinternen E-Mail-Server gestattet. Eine direkte Verbindung vom Arbeitsplatz-PC des Anwenders zu einem E-Mail-Server außerhalb des Unternehmens darf nicht aufgebaut werden
- Die Nutzung von Diensten, die Datentransfer zulassen, sollte streng kontrolliert und nur bei geschäftlicher Anforderung freigeschaltet werden
- Häufig wird durch Systeme an der Schnittstelle zum Internet überwacht, welche Internetseiten durch einen Anwender aufgerufen werden. Ebay & Co. werden dort häufig geblockt
- Durch geeignete Verfahren sollte die Verbindungsstrecke, das Routing, festgelegt werden können. So wird verhindert, dass Informationen über unsichere Netzwerkdienste laufen.

[11.5.] Zugriffskontrolle Betriebssystem

Ziel:

Schutz vor unbefugten Zugriffen auf ein Betriebssystem.

Maßnahmen:

- Jeder Zugriff auf ein Betriebssystem sollte durch ein sicheres Anmeldeverfahren geschehen
    - Passwörter dürfen nicht auf dem Bildschirm dargestellt werden
    - Benutzernamen sollten nicht vorbelegt sein
    - die Anzahl der maximal möglichen Anmeldeversuche sollte definiert sein, üblich sind hier drei
    - Passwörter sollten nicht unverschlüsselt übertragen werden
- Jeder Anwender sollte eine eigene und eindeutige Identität haben. Diese kann auch über den Besitz von Smartcards und Hardware-Token erfolgen
- Entsprechende Verfahren zur Authentifikation von Anwendern müssen etabliert sein. Authentifikation ist die Verifikation der Identität durch Wissen, also Passwort, PIN oder Passphrase. Biometrische Verfahren können hier ebenfalls eingesetzt werden, zum Beispiel Fingerabdruck, Iris-Scan oder Gesichtserkennung
- Erfolgreiche und fehlgeschlagene Zugriffe müssen protokolliert werden
- Eine Protokollierung von ausgewählten Systemprivilegien muss erfolgen
- Bei Verstößen gegen das Authentifikationsverfahren muss eine Alarmierung erfolgen
- Wo die Geschäftsanforderungen bestehen, kann auch ein zeitlich begrenzter Zugriff auf ein Betriebssystem erfolgen

- Die Verwendung von Systemprogrammen, die beispielsweise Protokolldateien verändern können, sollte so weit wie möglich ausgeschlossen werden. Wo diese benötigt werden, muss die Benutzung überwacht und sicher protokolliert werden
- Nicht benutzte Datenverbindungen (Session) sollten nach einer definierten Zeit automatisch beendet werden.

[11.6.] Zugriffskontrolle Software-Anwendungen

Ziel:

Schutz der Informationen in Software-Systemen vor unbefugten Zugriffen.

Maßnahmen:

- Nur befugte Anwender dürfen Zugriffsrechte zu Informationen in Software-Anwendungen erhalten
- Die Identität eines Anwenders muss festgestellt werden
- Die Authentizität eines Anwenders muss durch geeignete Verfahren sichergestellt werden
- Zugriffe zu Informationen in Software-Anwendungen sollten immer aufgrund einer Rolle gewährt werden
- Es muss festgelegt werden, welche Rechte ein Anwender in Bezug auf Informationen hat, also Schreib-, Lese-, Lösch- oder Ausführungsrechte.

[11.7.] Mobile Computing und Teleworking

Ziel:

Einhaltung der Sicherheitsziele bei Benutzung von Mobile Computing und Teleworking.

Maßnahmen:

- Der Schutz sollte den Risiken entsprechen, die durch den Einsatz der mobilen Technik entstehen
- Es müssen Regeln zum Umgang mit der mobilen Technik aufgestellt und Maßnahmen definiert werden, um die Informationen auf dem mobilen Systemen vor unbefugtem Zugriff, Veränderung oder Löschung zu schützen
- Mindestens müssen Zugriffskontrolle, sichere Kommunikation, Datenträgerverschlüsselung, Informationsbackup und Anti-MalWare implementiert sein
- Eine Benutzung von öffentlichen drahtlosen Netzwerken, so genannten Hotspots, sollte unterbunden werden
- Die Flexibilisierung der Arbeit durch Verlagerung aus Unternehmen heraus, dem Teleworking, sollte nur nach einer angemessenen Risikobewertung und bei etablierten Maßnahmen implementiert werden
- Beim Teleworking müssen geeignete Maßnahmen etabliert sein

    - zur Sicherstellung der Authentizität eines Anwenders
    - für eine sichere Kommunikationen, da genutzte Software-Anwendungen häufig sensible Informationen benötigen und diese nicht über öffentliche Netzwerke im Klartext übertragen werden dürfen
    - so dass Informationsbackups, beispielweise von lokal abgelegten Daten, wie Handakten, Notizen und Protokolldateien regelmäßig gesichert und wiederhergestellt werden können.

[12.2.] Funktionale Korrektheit von Software-Anwendungen

Ziel:

Vermeidung von Fehlern, Verlust, unbefugter Veränderung und Missbrauch von Informationen in Software-Anwendungen.

Maßnahmen:

- Funktional richtige Software bedeutet, dass ein guter Qualitätssicherungsprozess bei der Entwicklung und Implementierung von Software-Anwendungen aufgesetzt ist und ein konsequentes Testmanagement die definierten funktionalen Qualitätsmerkmale gewährleisten konnte.

Dieses steht nicht im Fokus von ITIL, so dass dieser Abschnitt nicht vertieft wird.

[12.3.] Verschlüsselung

Ziel:

Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen.

Maßnahmen:

- Je mehr Informationen über weite Strecken und unbekannte Netzwerke ausgetauscht werden, desto größer wird die Bedrohung, dass diese Information abgefangen, gelesen, verändert und wiederholt weitergeleitet wird. Dagegen sind geeignete Maßnahmen zu treffen
- Es müssen Regelungen zum Einsatz von Verschlüsselungsverfahren getroffen werden, die festlegen:
    - ob Verschlüsselungsverfahren genutzt werden dürfen
    - welche Verfahren genutzt werden müssen
    - welche Informationen verschlüsselt werden müssen und
    - wie bei einem Verstoß gegen das Verfahren gehandelt werden muss.

- Es muss ein Verfahren zur Schlüsselverwaltung implementiert sein, das sicherstellt wie Schlüssel erzeugt und gespeichert werden, wie diese verteilt, veröffentlicht und zurückgezogen werden und wie die Wiederherstellung von verlorenen oder beschädigten Schlüsseln erfolgen kann.

[12.4.] Sicherheit von Systemdateien

Ziel:

Schutz der Systemdateien vor unbefugtem Zugriff, Veränderung und Löschung.

Maßnahmen:

- Es sollten Verfahren implementiert sein, wie Betriebssysteme installiert und aktualisiert werden. Dieses wird bei ITIL durch das Release Management sichergestellt
- Dateien, die für Testsysteme benutzt werden, müssen anonymisiert werden, so dass die Vertraulichkeit sichergestellt wird
- Der Zugriff auf Source Code von Software-Anwendungen sollte eingeschränkt sein.

[12.5.] Sicherheit von Entwicklungs- und Wartungssystemen

Ziel:

Entwicklungs- und Wartungsumgebungen müssen überwacht werden, um den Schutz der Produktionsumgebung sicherzustellen.

Maßnahmen:

- Es muss sichergestellt sein, dass durch Entwicklung und Wartung das erreichte IS-Niveau gehalten und sogar verbessert werden kann
- Die Entwicklungs- und Wartungssysteme müssen denselben Verfahren unterliegen, die auch für die Produktivsysteme gelten

- Alle Änderungen an den CIs müssen identifiziert, genehmigt und dokumentiert werden. Diese Aufgabe übernimmt bei ITIL das Change Management
- Nach jeder Änderung müssen angemessene Tests durchgeführt werden, die sicherstellen, dass die Sicherheitsziele erfüllt werden. Beispielweise müssen durch geeignete Maßnahmen, zum Beispiel statische Code-Analysen, Hintertüren in dem Source Code gesucht werden
- Änderungen an Software-Anwendungen sollten auf die notwendigen Änderungen beschränkt sein
- Für Software-Anwendungen, die durch Dritte entwickelt werden, muss festgelegt werden, welche IS-Kriterien zur Abnahme gelten. Das Unternehmen, das die Entwicklung durchführt, muss sorgfältig ausgewählt und einer Risikoüberprüfung unterzogen werden. Eine Steuerung durch definierte Qualitätssicherungs- und Controllingverfahren muss implementiert werden.

[12.6.] Technische Schwachstellen

Ziel:

Das Risiko, dass durch bekannte technische Schwachstellen entsteht soll gemindert werden.

Maßnahmen:

- Informationen über aktuelle Schwachstellen sollten dem Unternehmen in angemessener Form zur Verfügung stehen, beispielsweise durch die Nutzung eines CERT-Dienstes[6], der Warnungen und Hinweise zu Schwachstellen sammelt und an seine Kunden verteilt
- Hinweise auf Schwachstellen, die durch Hersteller gemeldet werden und für die Patches angeboten werden, sollten auf ihre Authentizität überprüft werden. Ebenfalls sollten Patches immer aus gesicherten und bekannten Quellen geladen werden

[6] Computer Emergency Response Team

- Patches müssen wie Änderungen an Software-Anwendungen behandelt werden
- Jedes CI muss bekannt sein, damit eine optimale Risikobewertung vorgenommen werden kann und angemessene Maßnahmen daraus abgeleitet werden können.

[13] Security Incidents

Ziel:

Security Incidents und Schwachstellen müssen gemeldet werden, damit notwendige Maßnahmen so schnell wie möglich ergriffen werden können.

Maßnahmen:

- Eine Policy muss festlegen, was ein Security Incident ist. Weiterhin muss festgelegt werden, wie diese zu melden sind und welche Maßnahmen ergriffen werden müssen.

Der Umgang mit Security Incidents wird in Kapitel 3.4.1 Incident Management beschrieben.

[14] Business Continuity Management

Der Prozess, sowie die notwendigen Maßnahmen sind unter Kapitel 3.3.5 IT Service Continuity Management beschrieben.

5.5 Check

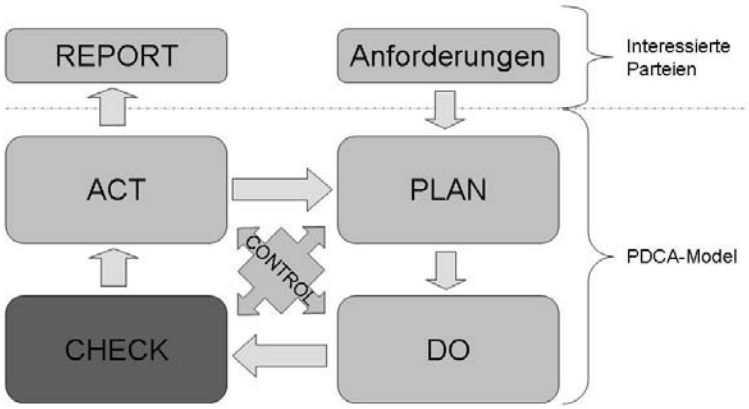


Abbildung 32: Security Maßnahmen - Check

Das Ziel der Check-Phase ist die Überprüfung von Maßnahmen auf Einhaltung oder Abweichung von den Anforderungen, sowie die Identifikation von Optimierungspotentialen. Die gefundenen Abweichungen und Optimierungspotentiale werden über die Act-Phase eingesteuert, so dass die Maßnahmen verbessert werden können. Über die Ergebnisse der Check-Phase werden Berichte erstellt, die durch die Report-Aktivität kommuniziert werden.

Für die Check-Aktivität sind durch ISO/IEC 17799:2005 nur wenige feste Prüfpunkte vorgegeben, jedoch muss jede eingesetzte Maßnahme regelmäßig überprüft werden. Die Häufigkeit ist abhängig von der Risikobewertung, die der Maßnahme zugrunde liegt.

[5] Security Policy

[5.1.] Information Security Policy

[5.1.2.] Regelmäßige Überprüfung der Security Policy

- Zur Überprüfung der Security Policy müssen folgende Quellen untersucht werden:

  - Rückmeldungen und Beschwerden von Externen
  - Ergebnisse unabhängiger Überprüfungen
  - Ergebnisse interner Überprüfungen
  - Trends über Bedrohungen und Schwachstellen
  - Auswertung von Security Incidents
  - Empfehlungen von Experten

[6] Organisation der IS

[6.1.] Interne Organisation

[6.1.8.] Unabhängige Überprüfung der IS

- Die interne Organisation der IS sollte regelmäßig auf seine Gültigkeit, Angemessenheit, Eignung und Effizienz hin überprüft werden
- Die Unternehmensleitung sollte diese Überprüfung initiieren
- Die Unabhängigkeit sollte durch organisatorisch unabhängige oder externe Experten sichergestellt werden. Dabei muss die Fachkunde der Experten gewährleistet sein.

[11] Zugriffskontrolle

[11.2.] Zugriffsrechte für Anwender

[11.2.4.] Überprüfung der Zugriffsrechte für Anwender

- Ein Verfahren muss definiert werden, mit dem Zugriffsrechte für Anwender regelmäßig überprüft werden können
- Die Häufigkeit dieser Überprüfung sollte von der Rolle und den Rechte abhängig sein
- Bei Änderungen des Beschäftigungsverhältnisses oder der Rolle sollte eine Überprüfung stattfinden
- Protokolldateien über Änderungen an Zugriffsrechten sollten ebenso untersucht werden wie die Systeme, auf denen Zugriffsrechte verwaltet werden.

5.6 Act

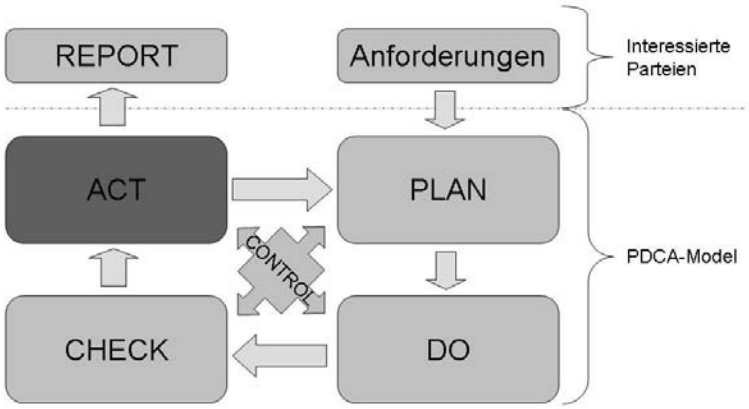


Abbildung 33: Security Maßnahmen - Act

Während der Act-Phase werden die gefundenen Optimierungspotentiale bewertet und bei Bedarf in Verbesserungsmaßnahmen umgesetzt. ISO/IEC 17799:2005 gibt hier Hinweise, wie mit gefundenen Schwachstellen und Verfahren, die nicht optimal implementiert sind, umgegangen werden sollte.

- Analyse der Ergebnisse aus der Check-Phase
- Herleitung von Verbesserungsmaßnahmen für die Security Pläne
- Analyse der SLA und OLA auf Optimierungspotentiale.

6 Fazit

Wachsende Bedrohungen für die Informationen betreffen uns alle. Die Art zu kommunizieren verändert sich rasant, immer mehr Informationen werden digital ausgetauscht. Die Gesellschaft hat eine neue Maxime entdeckt – „Allways On".

Dadurch verändert sich auch die Weise, wie gearbeitet wird. Plötzlich erscheint es uns als Freiheit, an einem warmen Sommertag das Notebook auf einer Picknickwiese aufzuklappen um schnell noch einmal E-Mails zu schreiben oder eine Präsentation vorzubereiten.

Durch die Verlagerung des Umgangs mit Informationen aus den Büros heraus wächst jedoch auch die Gefahr, dass ein unkontrollierter Informationsfluss stattfindet, also ein Security Incident auftritt.

Die Entwicklung der Skript-Kiddies und Hacker hin zu Kriminellen, die es auf das Geld ihrer Opfer abgesehen haben, lässt die Bedrohung nur noch schneller wachsen.

Neue Bedrohungen erfordern neue Maßnahmen. Das ist die Lehre, die uns die Hersteller von Sicherheitssystemen seit Jahren immer wieder predigen. Nun wächst die Zahl der eingesetzten Sicherheitssysteme, seien es Software-Anwendungen oder Hardware-Lösungen, aber ständig und es ist kein Ende der Bedrohung abzusehen.

Also muss erkannt werden, dass mit Sicherheitssystemen der Krieg gegen Security Incidents nicht gewonnen werden kann. Hier hilft nur eine prozessorientierte Herangehensweise, die eine Systematik in die Maßnahmen bringt, dadurch wiederverwendbare Verfahren und IS-Maßnahmen festlegt und alles in den Kontext mit anderen Prozessen bringt, die zentrale Aufgaben übernommen haben, beispielsweise die zentrale Prüfung und Freigabe von Änderungen.

Der weiße Ritter heißt hier ITIL, das alle notwendigen Prozesse in einen Kontext gebracht und daraus ein sinnvolles Rahmenwerk erstellt hat.

Das Security Management im ITIL-Kontext, das analog zu diesem Buch implementiert werden kann, bietet zum einen den Schutz der Informationen, stellt aber gleichzeitig sicher, dass eine Wirtschaftlichkeit erzielt wird, da die IS-Maßnahmen und Verfahren immer auf Basis der bestehenden Anforderungen geplant, implementiert und betrieben werden. Fällt eine Anforderung weg, kann auch die dazugehörige Maßnahme aussortiert werden. Das macht ITIL flexibel.

Ein weiterer großer Vorteil von ITIL ist die Standardisierung der Begriffe, so dass die Fachseite sich nicht hinter den Fachbegriffen und die IT-Seite sich nicht hinter den IT-Begriffen verstecken kann. ITIL versteht sich hier nicht als großer Gleichmacher, sondern eher als Dolmetscher zwischen den Welten.

Anhang A: Fragebogen zum ITIL Security Management

Die folgenden Fragen können mit Ja oder Nein beantwortet werden. In der dritten Spalte wird durch ein „M“ angezeigt, ob es sich um eine Muss-Anforderung handelt.

Level 1	**Voraussetzungen**	
Nr. 1	Hat die Unternehmensleitung die Notwendigkeit der IS erkannt und unterstützt sie diese?	M
Nr. 2	Sind die Anforderungen an die IS aus Geschäftssicht identifiziert und dokumentiert?	M
Nr. 3	Gibt es eine IS-Policy oder andere übergeordnete Dokumente, welche die IS-Ziele definieren und deren Wichtigkeit für das Unternehmen herausstellen?	
Nr. 4	Sind bereits Security Management Aktivitäten in dem Unternehmen etabliert?	
Nr. 5	Sind die Aktivitäten vom Security Management bestimmten Personen oder Funktionsbereichen zugeordnet?	
Nr. 6	Sind Maßnamen implementiert, Security Incidents zu identifizieren?	

Level 1.5	**Unternehmensausrichtung**	
Nr. 7	Sind Zweck und Vorteile des Security Management in der Organisation bekannt?	M
Nr. 8	Sind die Sicherheitsziele im Unternehmen bekannt?	M
Nr. 9	Sind alle Anwender darauf verpflichtet, die Sicherheitsziele und die Maßnahmen des Security Managements einzuhalten?	M
Nr. 10	Werden die Anwender aktiv in das Security Management einbezogen?	

Level 2	**Prozesstauglichkeit**	
Nr. 11	Sind die Verantwortlichkeiten für die Aktivitäten des Security Managements zugeordnet?	M
Nr. 12	Ist die Aufgabe des Security Managements in der Organisation etabliert?	M
Nr. 13	Gibt es Verfahren, um Risiken vergleichbar und einheitlich zu bewerten?	M

Nr. 14	Gibt es Verfahren, um die Security Incidents festzustellen, zu analysieren und vorherzusagen?	
Nr. 15	Können Verstöße gegen IS-Ziele sanktioniert werden?	
Nr. 16	Gibt es Verfahren zum Planen, Überwachen und Messen von vertraglich definierten Sicherheitszielen?	
Nr. 17	Werden alle Security Incidents analysiert?	
Nr. 18	Sind Ziele für die Qualitätsmerkmale Verfügbarkeit, Vertraulichkeit und Integrität definiert und sind diese festgelegt in SLAs, OLAs und UC?	
Nr. 19	Werden Informationen Klassifiziert?	
Nr. 20	Werden Bedrohungen analysiert und geeignete Maßnahmen ergriffen?	

Level 2.5	**Interne Integration**	
Nr. 21	Werden die Anforderungen der Kunden in das Security Management miteinbezogen?	M
Nr. 22	Ist das Security Management für alle Verfahren und IS-Maßnahmen verantwortlich?	M
Nr. 23	Analysiert das Security Management Auditergebnisse und Security Incidents analysiert und daraufhin Verbesserungen von Maßnahmen eingeleitet?	M

Level 3	**Produkte**	
Nr. 24	Werden regelmäßig Berichte erstellt, welche die Erreichung der IS-Ziele betreffen?	M
Nr. 25	Gibt es Security Pläne und werden diese regelmäßig geprüft?	

Level 3.5	**Qualitätskontrolle**	
Nr. 26	Sind die Verfahren und Qualitätskriterien, die auf das Security Management anwendbar sind, klar und werden sie angewendet?	M
Nr. 27	Sind die Aufgaben des Security Management entsprechend geschult worden?	
Nr. 28	Sind die Anwender hinsichtlich der IS-Ziele geschult und wird die Eignung der Anwender überprüft?	
Nr. 29	Hat die Organisation Ziele für das Security Management gesetzt und kontrolliert sie diese?	
Nr. 30	Hat die Organisation Richtlinien für das Security Management gesetzt und kontrolliert sie diese?	
Nr. 31	Nutzt die Organisation angemessene Werkzeuge zur Unterstützung des Security Managements?	

Level 4	**Berichtswesen**	
Nr. 32	Gibt es Berichte über Security Incidents (Häufigkeit, Art, Umfang, Schaden)	M
Nr. 33	Gibt es Berichte über definierte Messpunkte (KPIs)	
Nr. 34	Gibt es ein Verfahren, dringende Security Incidents sofort zu berichten?	
Nr. 35	Gibt es Berichte über die Effizienz von Maßnahmen?	
Nr. 36	Gibt es Berichte über Schulungsbedarf in Bezug auf IS?	

Level 4.5	**Externe Integration**	
Nr. 37	Werden regelmäßig Meetings mit allen beteiligten Prozessen durchgeführt, in denen Belange des Security Managements diskutiert werden?	M
Nr. 38	Tauscht das Security Management Informationen mit dem Incident Management aus, beispielsweise bezüglich Security Incidents, Priorisierungen und Workarounds?	
Nr. 39	Tauscht das Security Management Informationen mit dem Problem Management aus, beispielsweise bezüglich Schwachstellen, notwendigen RfCs und Root Cause Analysen?	
Nr. 40	Tauscht das Security Management Informationen mit dem Configuration Management aus, beispielsweise bezüglich Richtlinien zur Klassifikation von Informationen, Lizenzbestimmungen und Anforderungen an IS Kriterien in der CMDB?	
Nr. 41	Tauscht das Security Management Informationen mit dem Change Management aus, beispielsweise bezüglich Abnahmekriterien und Changes?	
Nr. 42	Tauscht das Security Management Informationen mit dem Release Management aus, beispielsweise bezüglich Tests, Rolloutplanungen und der Anforderungen an die DSL?	
Nr. 43	Tauscht das Security Management Informationen mit dem Service Level Management aus, beispielsweise bezüglich Anforderungen von Kunden, notwendigen Berichten und der Kommunikation mit dem Kunden?	

Nr. 44	Tauscht das Security Management Informationen mit dem Availability Management aus, beispielsweise bezüglich Planung und Überwachung der Verfügbarkeit von IT-Services?	
Nr. 45	Tauscht das Security Management Informationen mit dem Capacity Management aus, beispielsweise bezüglich der IT-Roadmap und den Risikotrends?	
Nr. 46	Tauscht das Security Management Informationen mit dem Finance Management aus, beispielsweise bezüglich RoI und TCO von IS-Maßnahmen und Verfahren?	
Nr. 47	Tauscht das Security Management Informationen mit dem Continuity Management aus, beispielsweise bezüglich Anforderungen an die IS während Notfällen?	

Level 5	**Schnittstelle zum Kunden**	
Nr. 48	Wird mit dem Kunden überprüft, ob die vom Security Management durchgeführten Aktivitäten optimal sein Geschäft unterstützen?	M
Nr. 49	Werden Trends in der Kundenzufriedenheit bezüglich der IS aktiv überwacht?	

Glossar

Anti-MalWare Programm

Programm zum Schutz vor, sowie zur Erkennung und Entfernung von MalWare.

Audit

Überprüfung auf Einhaltung von Verfahrensanweisungen.

Ausfallsicherheit

Sicherheit eines Systems oder eines IT-Services vor einem Ausfall.

Authenticity

Siehe Authentizität

Authentizität

Authenticity; Sichere (authentisierte) Zuordnung eines Anwenders zu einer Identität.

Backout

Ein Backout ist ein Verfahren, die einzelnen Changes eines Releases schrittweise rückgängig zu machen. Durch ein Backout wird ein neues Re-lease definiert.

BASEL II

Eigenkapitalvorschriften, zur Sicherstellung einer angemessenen Ausstattung mit Eigenkapital sowie zur Vereinheitlichung von Kreditvergaberichtlinien.

Benchmark

Verfahren zum Vergleich von definierten Leistungsmerkmalen. Um ein Benchmark durchführen zu können, ist es wichtig, eine Beurteilungsbasis zu haben, die eine Vergleichbarkeit ermöglicht. Hier eignen sich besonders Standardisierte Rahmenwerke, wie beispielsweise ITIL.

Best Practice

Verfahren, die sich bereits in zahlreichen Unternehmen in der Praxis bewährt haben, und somit als Musterlösungen für andere Unternehmen angesehen werden können.

BSI Grundschutzhandbuch

Eigentlich IT-Grundschutzhandbuch; dieses enthält Standardsicherheitsmaßnahmen und Umsetzungshinweise für die IT. Das IT-Grundschutzhandbuch ist für alle Bundesbehörden verbindlich.

CERT

Computer Emergency Response Teams (CERTs) oder im Deutschen Computer-Notfallteams gibt es seit 1988. Ihre Aufgabe besteht in der Unterstützung Betroffener, wenn ein Sicherheitsvorfall (engl.: Incident) auftritt.

[Quelle: Klaus-Peter Kossakowski]

Change

Änderung

Code of Practice

Verfahrensregeln

Cold Standby

Backup-Verfahren, bei dem die Infrastruktur bereits vorbereitet, aber noch nicht installiert ist. Beispielsweise ein Rechenzentrum, das im Notfall noch mit Systemen und Peripheriegeräten ausgestattet werden muss.

Commercial-off-the-Shelf

Auch CotS genannte Software-Anwendungen, die "direkt aus dem Verkaufsregal", also ohne aufwändige Anpassung auf eigene Bedürfnisse, effizient und effektiv genutzt werden können.

Compliance

Einhaltung von Vorgaben, Gesetzen, Richtlinien, Verfahrensregeln, etc.

Configuration Items

Configuration Items (Konfigurationselemente, CI) sind IT-Systeme, wie zum Beispiel Server und Arbeitsplatz-PC, Peripheriegeräte, wie zum Beispiel Drucker und Scanner, aber auch Handbücher, Netzwerkkomponenten und Datenträger verstanden.

Configuration Management Database (CMDB)

Datenbank, in der alle Configuration Items abgelegt werden.

Definitive Hardware Store (DHS)

Der Definitive Hardware Store ist ein Lager, das sämtlich genehmigte Hardwaresysteme und Ersatzteile enthält.

Definitive Software Library (DSL)

Die Definitive Software Library ist ein Archiv, in der alle genehmigten und aktuellen Softwareversionen vorgehalten werden. Diese DSL ist häufig ein Teil der CMDB.

Due Diligence

Unter einer Due Diligence versteht man eine Prüfung, um den Wert eines Unternehmens zu ermitteln.

Fallback

Ein Fallback ist die Wiederherstellung der vorherigen Releases. Dadurch werden alle Changes, die in einem Release zusammengefasst waren, rückgängig gemacht.

Firewall

Als Firewall oder Zugangsschutz(system) bezeichnet man bei Rechnernetzen ein organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege.

[www.wikipedia.de]

GDPdU

Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) regeln, dass das Finanzamt elektronische Steuerprüfungen vornehmen darf. Durch die GDPdU werden die Pflichten der Unternehmen geregelt.

Hacker

Computerspezialist, der IS-Maßnahmen umgehen oder überwinden kann, und somit unbefugten Zugang zu Netzwerken und fremden Systeme sowie Zugriff zu Informationen erlangen kann.

Integrität

Integrität (engl. Integrity) stellt das Maß dar, in dem Informationen richtig gespeichert sind, verarbeitet oder übertragen werden. Richtig bedeutet hier, dass die Informationen nicht unbefugt und unbeabsichtigt verändert werden, wie dieses beispielsweise MalWare tut.

Intrusion-Detection

Erkennen eines unbefugten Zuganges zu einem Netzwerk oder System, beziehungsweise eines unbefugten Zugriffs auf Informationen.

Intrusion-Prevention

Verhinderung von unbefugten Zugängen zu Netzwerken oder Systemen, beziehungsweise von unbefugten Zugriffen auf Informationen. Der Verhinderung (Prevention) geht immer eine Erkennung (Detection) voraus. Daher gelten Systeme zur Intrusion-Prevention als "Nachfolger" von Intrusion-Detection Systemen.

ITIL

Die Information Technology Information Library ist ein Best Practice (de facto) Standard für die Erbringung von IT-Services (IT-Betriebsprozesse).

IT-Service

IT-Dienstleistung

MalWare

Langform von Malicious Software (Bösartige Software); Gruppenbegriff für Viren, Würmer und Trojaner.

Non-Repudiation

siehe Unleugbarkeit

Operational Service Agreement (OLA)

Durch ein Operational Service Agreement werden die Service-Vereinbarung mit den internen Leistungserbringern geregelt.

Österreichisches IT-Sicherheitshandbuch

Sicherheitsrichtlinie analog zum IT-Grundschutzhandbuch, allerdings auf Österreichische Normen und Gesetze ausgelegt.

PDCA-Modell

Plan-Do-Check-Act; Modell nach W. Deming für einen sich selbst optimierenden Prozesskreislauf.

Pentest

Penetrationstest; Versuch, mit den Methoden eines Hackers unbefugten Zugang zu Netzwerken oder auf Systemen zu erlangen, und somit Zugriff zu Informationen.

Restore

Wiederherstellung eines bestimmten Zustandes, meist die Wiederherstellung der letzten Datensicherung.

Security by Obscurity

Prinzip der „Sicherheit durch Verschleierung“ bei dem angenommen wird, dass Verfahren und Methoden nicht bekannt sein dürfen, um Sicherheit zu erhalten.

Security Incident

Sicherheitsvorfall; Störung der Informationssicherheit

Security Section

Abschnitt des SlAs, in der Anforderungen eines Kunden an die IS von IT-Services definiert sind.

Segregation of Duties

Trennung der Verantwortlichkeit

Service Delivery

Unter Service Delivery werden bei ITIL die taktischen IT-Betriebsprozesse verstanden.

Service Level Agreement

Vereinbarung über Qualität und Quantität einer zu erbringenden Dienstleistung.

Service Level Requirements for Security

Die Service Level Requirements (SLR) for Security sind die Anforderungen eines Kunden an die IS.

Service Support

Unter Service Support werden bei ITIL die operativen IT-Betriebsprozesse verstanden.

Servicefähigkeit

Die Servicefähigkeit (engl. Serviceability) beschreibt, wie die Unterstützung durch Dritte in Bezug auf die Verfügbarkeit, Wartbarkeit und Zuverlässigkeit der Komponenten gewährleistet ist, die unter der Verantwortung dieser Dritten stehen.

Service-Katalog

Liste aller IT-Dienstleistungen, die ein IT-Dienstleister als Standard-Dienstleistung erbringen kann.

Social Engineering

Prüfung von persönlichem Verhalten von Anwendern in Bezug auf Sicherheitsziele und Verfahren.

Tool

Dienstprogramm, in der Regel eine Software-Anwendung, die spezielle Aufgaben wahrnehmen, wie beispielsweise Bekämpfung von MalWare.

Trojaner

Ein "Trojanisches Pferd" ist ein (ausführbares) Programm, dem unerkannte zusätzliche Funktionen aufgeprägt sind.

[Quelle: Brunnstein, Computer-Viren-Report]

Trustworthiness

Siehe Vertrauenswürdigkeit

Underpinning Contract

Underpinning Contracts (UC), sind Verträge, welche die Einbindung von externen Partnern regelt wie beispielsweise Hardwarelieferanten oder externen Systemexperten.

Unleugbarkeit

Non-Repudiation; Stellt sicher, dass ein Versender eine Information auch tatsächlich verschickt hat (Non-Repudiation of Origin) und dieses später nicht leugnen kann. Ebenso muss auch sichergestellt werden, dass ein Empfänger eine Information auch tatsächlich erhalten hat (Non-Repudiation of Delivery), und dieses später nicht abstreiten kann.

Verfügbarkeit

Die Verfügbarkeit (engl. Availability) beschreibt den Grad, inwiefern IT-Service in einem definierten Zeitraum zur Nutzung zur Verfügung stehen.

Vertrauenswürdigkeit

Eigenschaft, die den Grad beschreibt, wie eine erwartete Funktionalität auch tatsächlich erbracht wird.

Vertraulichkeit

Vertraulichkeit (engl. Confidentiality) bedeutet, dass nur berechtigte Personen und Systeme auf Informationen Zugriff erhalten.

Virus

Ein Computer-Virus ist ein unselbständiges Programmstück, das sich (wahlfrei oder gezielt) durch Replikationsmechanismen an Software-Anwendungen, Dokumente oder Betriebssysteme anhängt. Es kann sich durch Selbstverschlüsselung oder andere Maßnahmen tarnen, und durch Mutation sein Aussehen stark verändern. Computer-Viren rufen typischerweise Wirkungen (Payloads, Schadensfunktionen) hervor, wobei entweder vorübergehende oder dauerhafte Schäden beobachtet werden. [Quelle: Brunnstein, Computer-Viren-Report]

Wurm

Bei einem Computer-Wurm werden in einen vernetzten Computer zusätzliche Systemfunktionen über das Netzwerk hinzugefügt. [..] Der Name Wurm wird daraus abgeleitet, dass diese Programme einzeln "lebensfähig" und fortpflanzungsfähig sind. [Quelle: Brunnstein, Computer-Viren-Report]

Literaturverzeichnis

[A-SIT]

IKT-Stabsstelle des Bundes

Das Österreichische IT-Sicherheitshandbuch

Wien, 2003

[Brunnstein, K., 1991]

Prof. Dr. Klaus Brunnstein

Computer-Viren-Report

Gefahren, Wirkungen, Aufbau, Früherkennung, Vorsorge

2. Auflage

Hamburg, 1991

[Brunnstein, K., 2001]

Prof. Dr. Klaus Brunnstein

IT Security and Safety Curriculum

Universität Hamburg

Hamburg, 1989 - 2001

[BSI, 2004]

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutzhandbuch

Version 2004

Bonn, 2004

[ISO, 2005]

ISO/IEC 27001:2005

Information Security Management System - Requirements

Genf, 2005

ISO/IEC 17799:2005
Information Security Management System – Code of Practice
Genf, 2005

[Nader, R., 1965]
Ralph Nader
Unsafe at any Speed
2. Auflage
New York, 1965, 1972

[OGC]
Office of Government Commerce
Best Practice for Security Management
UK, 1999 - 2004

Office of Government Commerce
ITIL – The Key to Managing IT Services
Service Deliver Version 2.0
UK, 2003

Office of Government Commerce
ITIL – The Key to Managing IT Services
Service Support Version 2.0
UK, 2003

[Olbrich, A., 2004]
Alfred Olbrich
ITIL kompakt und verständlich
2. Auflage
Aschaffenburg, 2004

[Victor, F.; Günther, H., 2005]
Frank Victor, Holger Günther
Optimiertes IT-Management mit ITIL
2. Auflage
Aachen und Bonn, 2004

Quellenverzeichnis Internet

[A-SIT]
http://www.a-sit.at
A-SIT Zentrum für sichere Informationstechnologie – Austria

[BSI]
http://www.bsi.de
Bundesamt für Sicherheit in der Informationstechnik

[ITIL]
http://www.itil.co.uk
Offizielle ITIL Internetseite

[itSMF]
http://www.itsmf.com
IT Service Management Forum

http://www.itsmf.de
IT Service Management Forum Deutschland e.V.

[KOSSAKOWSKI]
http://www.kossakowski.de/glossar.htm
CERT Experte

[OGC]

http://www.ogc.gov.uk

Office of Government Commerce

[UNI HAMBURG]

http://agn-www.informatik.uni-hamburg.de/

Universität Hamburg, Fachbereiche Informatik, Arbeitsbereich Anwendungen der Informatik in Geistes- und Naturwissenschaften (AGN)

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Change Advisory Board
CBT	Computer Based Training
CCTA	Central Computer and Telecommunications Agency
CERT	Computer Emergency Response Team
CI	Configuration Item
CMDB	Configuration Management Database
CRAMM	CCTA Risk Analysis and Management Methodology
CotS	Commercial-off-the-Shelf
DHS	Definitive Hardware Store
DRM	Digital Rights Management
DSL	Definitive Software Library
EDI	Electronic Data Interchange
Etc.	Et Cetera
GI	Gesellschaft für Informatik
GDPdU	Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
IPW	Implementation of Processed-oriented Working
IS	Informationssicherheit, Information Security
ISMS	Information Security Management System
IT	Informationstechnologie, Information Technology
ITIL	IT Infrastructure Library
ITSC	IT-Service Continuity
ItSMF	IT Service Management Forum
KPI	Key Performance Indicator
MP3	MPEG Audio Layer 3
MPEG	Moving Picture Experts Group
MWZ	Maximale Wiederanlaufzeit
OGC	Office of Government Commerce
OLA	Operational Level Agreement

PDCA	Plan – Do – Check – Act
PC	Personal Computer
QM	Qualitätsmanagement
QS	Qualitätssicherung
RfC	Request for Change
SLA	Service Level Agreement
TÜV	Technischer Überwachungsverein
UC	Underpinning Contract
UML	Unified Modelling Language
USB	Universal Seriel Bus
VDI	Verein Deutscher Ingenieure
VTL	Virtual Tape Library

Abbildungsverzeichnis

Tabellenverzeichnis

Sachwortverzeichnis

N

O

P

Q

R

S

T

U

V

W

Z