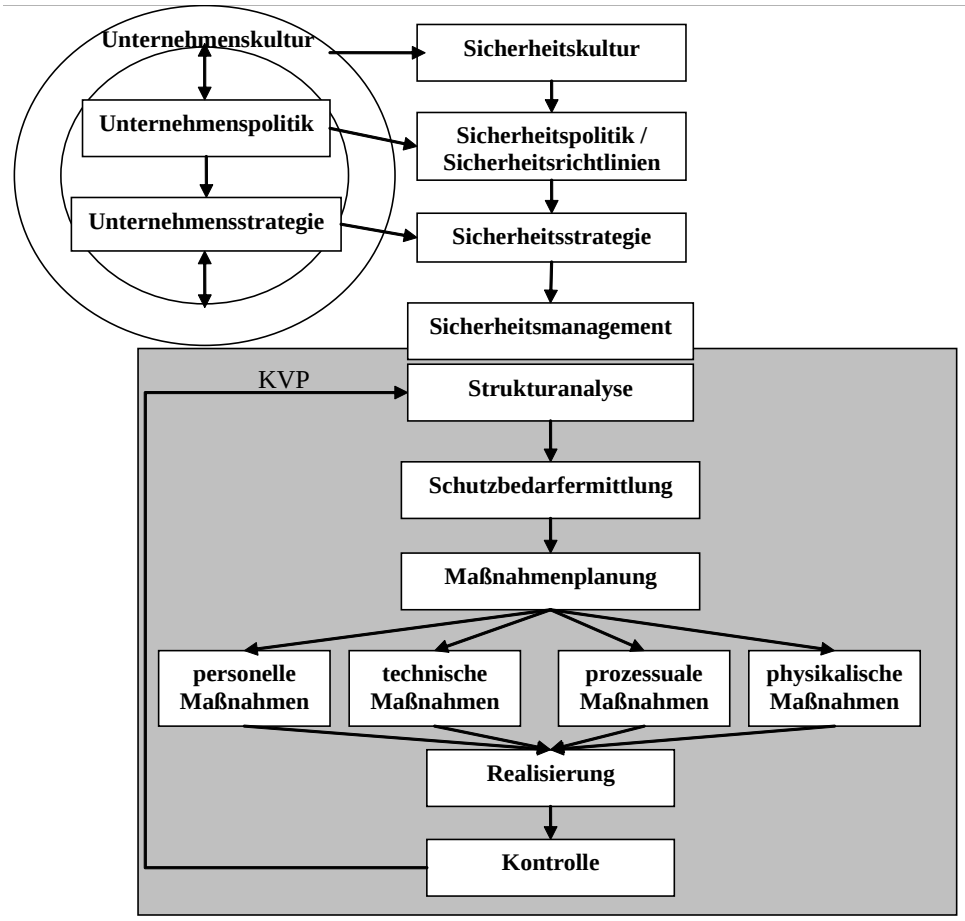
IWI Diskussionsbeiträge
39 (03. Februar 2010)[1]

ISSN 1612-3646

Ein ganzheitliches Konzept für Informationssicherheit unter besonderer Berücksichtigung des Schwachpunktes Mensch

Björn Semmelhaack[2], **Jon Sprenger**[3] und **Michael H. Breitner**[4]



[1] Kopien oder eine PDF-Datei sind auf Anfrage erhältlich: Institut für Wirtschaftsinformatik, Leibniz Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).

[2] Diplom-Ökonom, NORD/LB, Friedrichswall 10, 30159 Hannover (bjoern.semmelhaack@nordlb.de).

[3] Diplom-Ökonom, wissenschaftlicher Mitarbeiter und Doktorand (sprenger@iwi.uni-hannover.de).

[4] Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre und Direktor des Instituts für Wirtschaftsinformatik der Leibniz Universität Hannover (breitner@iwi.uni-hannover.de).

Abbildungsverzeichnis

Tabellenverzeichnis

1 Notwendigkeit der Informationssicherheit in einem Unternehmen

Informationen und Daten sind ein sensibler Faktor eines Unternehmens. Schutzmaßnahmen der Informationstechnik (IT) werden jedoch in vielen Unternehmen vernachlässigt.[5] Es bedarf einer adäquaten Informationssicherheit, die garantiert, dass Informationen verfügbar sind, jedoch lediglich für autorisierte Stellen.

Informationssicherheit besteht aus der IT-Sicherheit (Informations- sowie Datenschutz) und aus dem Schutz der IT-Technik. Zur Informations- und Datenverarbeitung werden Hardware- und Softwarekomponenten, Netzwerke sowie Menschen eingesetzt, die Schutz bedürfen. Der Mensch muss in ein geeignetes Sicherheitskonzept eingebunden werden, da der Mitarbeiter ein Risiko darstellt.[6] Mitarbeiter lassen sich idealtypisch in Menschenbilder eingruppieren,[7] so dass entsprechend differenziert auf diese eingegangen werden kann.

Informationssicherheit gilt es in der Unternehmenskultur zu verankern und in eine Sicherheitskultur einzubetten. Essentiell für die Informationstechnologie ist es, eine IT-Sicherheitsstrategie zu entwickeln.[8]

2 Basisanforderungen an die Informationssicherheit

Tabelle 1: Definitionen und rechtliche Grundlagen

Sicherheit	*Sicherheit* bezeichnet „den Zustand des Sicherseins vor Gefahr oder Schaden bzw. einen Zustand, in dem Schutz vor Gefährdungen besteht. […] Die Sicherheit zu einem bestimmten Zeitpunkt wird als **Ist-Sicherheit** bezeichnet und ist von einem geplanten Ausmaß an Sicherheit, der **Soll-Sicherheit**, zu unterscheiden.“[9]
***Informationssicherheit* (engl. security)**	*Informationssicherheit* (engl. security) beschreibt „die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.“[10]
Datensicherheit	*Datensicherheit* definiert „die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen. Damit umfasst die so beschriebene Sicherheit der Daten insbesondere auch Maßnahmen zur Datensicherung (engl. backup), also den Schutz vor Datenverlust durch Erstellung von Sicherheitskopien.“[11]
IT-Sicherheit	„Sicherheit in der Informationstechnik […] bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen • in informationstechnischen Systemen oder Komponenten oder • bei der Anwendung von informationstechnischen Systemen oder Komponenten“.[12] Nach dieser Definition bezweckt die IT-Sicherheit, durch rechtliche, technische und organisatorische Maßnahmen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Informationen bzw. Daten sicherzustellen.[13]
Compliance	„Übereinstimmung mit geltenden Vorgaben.“[14] Die Compliance wird von der Unternehmensführung vorangetrieben. Ziel ist die Einhaltung gesetzlicher Vorschriften und interner Vorgaben oder Beschlüssen von Aufsichtsbehörden.

[5] Vgl. Lassmann (2006), S. 349.
[6] Vgl. Schlienger (2007), S. 487; Mix/Pingel (2007), S. 498; Zerr (2007), S. 519; Fox (2003), S. 676; Schimmer (2007), S.510; Baier/Straub (2005), S. 313; Fox/Kaun (2005), S. 329; Schultz (2005), S. 426.
[7] Vgl. Schein (1980), S. 52.
[8] Vgl. von Solms/von Solms (2004), S. 372.
[9] Hoppe/Prieß (2003), S. 23 (Hervorhebungen im Original).
[10] Eckert (2008), S. 5.
[11] Ebenda.
[12] BSI-Einrichtungsgesetz vom 17. Dezember 1990 (BGBI I S. 2834), zuletzt geändert 2003 (BGBI. I S 2304).
[13] Vgl. Reinhard (2007), S. 37.
[14] Pohlmann (2008), S. 1.

Je nach Anforderungen an die Sicherheit zählen zu den wichtigsten Gesetzen das Bundesdatenschutzgesetz (BDSG), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das Telekommunikationsgesetz (TKG), die Telekommunikationsüberwachungsverordnung (TKÜV), das Signaturgesetz (SigG), die Fernüberwachungsverordnung (FÜV)[15] aber auch der Sarbanes Oxley Act (SOX) aus den USA[16].
Ziel des BDSG ist der Schutz von personenbezogenen Daten und nicht der Schutz sämtlicher Daten. Dabei sind personenbezogene Daten nicht allein auf den Menschen an sich beschränkt, sondern umfassen auch Aussagen über Sachen, solange ein unmittelbarer Bezug zwischen Sache und Person besteht. Zur Nutzung und Verarbeitung der Daten ist ein Unternehmen nur berechtigt, solange ein Gesetz dies erlaubt oder der Involvierte zugestimmt hat.[17]
Um die geltenden Vorschriften und Gesetze eines Unternehmens ordnungsgemäß „zu leben" bedarf es einer Sicherheitsstrategie und der dazugehörigen Sicherheitsziele.

2.1 IT-Sicherheitsstrategie

„Die Sicherheitsstrategie (engl. *security policy*) eines Systems oder einer organisatorischen Einheit legt die Menge von technischen und organisatorischen Regeln, Verhaltensrichtlinien, Verantwortlichkeiten und Rollen sowie Maßnahmen fest, um die angestrebten Schutzziele zu erreichen."[18] Die Sicherheitsstrategie eines Unternehmens lässt sich in systembestimmte und benutzerbestimmbare Anteile untergliedern, dabei sind die systembestimmten Anteile globale Regelungen, die z. B. vom Management oder einer anderen zuständigen Einheit festgelegt werden. Eine Klassifizierung der Sicherheitsstrategie wäre in den Informationssicherheitsklassen „öffentlich", „geheim" und „streng geheim" möglich sowie in eine Einteilung von Objekten und Subjekten in eben diese Sicherheitsklassen, wobei die Nutzer differenzierte Zugriffsrecht erhalten (mandatorische Strategie). Daneben existieren ferner rollenbasierte Strategien, welche die Zugriffe auf Objekte durch festgelegte Rollen reglementieren. Rollen beschreiben Aufgaben sowie die nötigen Berechtigungen und Verantwortlichkeiten.
Die Sicherheitsstrategie dient darüber hinaus der Festlegung von Maßnahmen, die zu ergreifen sind, wenn Risiken vermieden oder verringert werden sollen:[19]

- „Vorbeugung (Prävention), Pflege, Übung und Überprüfung (Verifikation)
- Beobachtung (Monitoring), Erkennung (Detektion), Meldung/Alarmierung
- Erwiderung (Reaktion), z. B. Abwehr
- Beurteilung (Evaluation) des Schadens
- Wiederherstellung (Restauration)
- Verbesserung (Emendation)"[20]

Zur Umsetzung der IT-Sicherheitsstrategie müssen Sicherheitsziele für das gesamte Unternehmen bzw. für bestimmte Bereiche definiert werden.

[15] Vgl. Krampert (2003), S. 23.
[16] Vgl. Schmidt (2007), S. 493f.
[17] Vgl. Pohl (2007), S. 55-59.
[18] Eckert (2008), S. 31 (Hervorhebung im Original).
[19] Vgl. Müller (2005), S. 93.
[20] Ebenda, S. 93.

2.2 IT-Sicherheitsziele

Um die Sicherheit von computergestützten Systemen zu gewährleisten, gilt es Ziele zu formulieren. Diese strategischen Sicherheitsziele werden zunächst durch das Top-Management des Unternehmens formuliert und folgend auf operativer Ebene präzisiert sowie umgesetzt. Letztlich wird ein Sicherheitssystem erstellt, das auf dem unternehmensweiten Sicherheitskonzept beruht.[21] Die fünf Hauptziele werden folgend erläutert:[22]

- *Verfügbarkeit* (engl. availability) „eines Systems ist gegeben, wenn keine Beeinträchtigung der Funktionalität eines IS vorliegen und das System einschließlich der Daten autorisierten Nutzern uneingeschränkt zur Verfügung steht.“[23] Ziel ist, die Nutzung, Funktionalität und Leistung der Systeme zu jeder Zeit zu garantieren, wobei die Verarbeitung von Daten und der Zugriff auf diese ausschließlich dem autorisierten Personal zustehen.[24]
- *Integrität* (engl. integrity) ist gewährleistet, „wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.“[25] Sie ist gegeben, falls übertragene und gespeicherte Daten vollständig und unverändert sind (Datenintegrität). Daneben ist das unbefugte Ändern von Funktionen (Funktionsintegrität) und Programmen (Programmintegrität) zu unterbinden, hierbei soll eine absichtliche Manipulation von fingierten, falschen oder unvollendeten Prozessen und Ergebnissen verhindert werden.[26]
- *Vertraulichkeit* (engl. confidentiality): besagt, dass nur Personen mit Autorisierung zum Datenzugriff und Systemzugang berechtigt sind. Die Daten und Systeme können durch verschiedene Vertraulichkeitsgrade geschützt werden.[27] Ein unbefugter Informationsgewinn durch ein unberechtigtes Einsehen der Daten soll unterbunden werden,[28] indem nur ein definierter Personenkreis Zugriff auf die Daten und Systeme erhält.[29]
- *Authentizität* (engl. authenticity) beschreibt, dass Personen, die Daten verarbeiten, erstellen und übertragen, auch ohne Zweifel als diese Person identifiziert werden können.[30]
- *Verbindlichkeit* (engl. non-repudiability): ist „in einem IS gewährleistet, wenn Authentizität und Nachweisbarkeit gegeben sind.“[31]

Zwischen den genannten Zielen bestehen Wechselwirkungen. Weiterhin sind Abhängigkeiten mit ökonomischen (Wirtschaftlichkeit) und sozialen Zielen (Akzeptanz) zu berücksichtigen,[32] die eine Umsetzung der Ziele verkomplizieren oder/und verteuern können.

2.3 IT-Sicherheit als Service

Der Einsatz der IT zur Erreichung der Unternehmensziele ist essentiell für eine Unternehmung, dabei liegt die Priorität nicht auf der Technik sondern auf den *IT-Services*. Diese sorgen im Zusammenspiel mit der Technik für eine konsequente Unterstützung der Geschäfts-

[21] Vgl. Heinrich et. al (2007), S. 173.
[22] Vgl. im Folgenden Eckert (2008), S. 6-12; Heinrich et. al (2007) S. 173-174; Gabriel (2006), S. 442-443; Hoppe/Prieß (2003), S. 24-25; Poguntke (2007), S. 6.
[23] Hoppe/Prieß (2003), S. 24.
[24] Vgl. Gabriel (2006), S. 442.
[25] Eckert (2008), S. 7.
[26] Vgl. Gabriel (2006), S. 442.
[27] Vgl. Hoppe/Prieß (2003), S. 24.
[28] Vgl. Gabriel (2006), S. 442.
[29] Vgl. Heinrich et al. (2007), S. 173.
[30] Vgl. Hoppe/Prieß (2003), S. 25.
[31] Hoppe/Prieß (2003), S. 25.
[32] Vgl. Gabriel (2006), S. 443.

prozesse, damit die IT-Dienstleistungen insgesamt effizient, effektiv und kundenorientiert ausgeführt werden können. Ein entscheidender Faktor für die Produktivität und Flexibilität und damit auch für die Produkt- oder Dienstleistungsqualität eines Unternehmens ist der Einsatz einer Informationstechnologie, die leistungsfähig, zuverlässig, flexibel, leicht benutzbar und auch sicher ist.[33]

IT-Services sind „Dienstleistungen, die dem Benutzer zur informationstechnischen Unterstützung der Geschäftsprozesse eines Unternehmens zur Verfügung gestellt werden“[34] und „die der Kunde als geschlossene Einheit wahrnimmt.“[35]Sollten IT-Services länger ausfallen, kann es bei einer Unternehmung zu großen Umsatzeinbußen bis hin zur Insolvenz kommen.[36]

Das *IT-Service Management (ITSM)* spezifiziert die einzelnen Services der Fachabteilungen und sorgt für deren reibungslosen Ablauf. Daneben werden Berichte erfasst, die über die Erfüllung der Services und deren Qualität Auskunft geben.[37] Die Kundenorientierung steht beim ITSM im Mittelpunkt, so dass die Qualität und Quantität der IT-Services ständig an die Kundenbedürfnisse neu anzupassen und zu optimieren sind.[38] Zur Einführung und Nutzung eines ITSM eignet sich der De-facto-Standard ITIL (IT Infrastructure Library), der ein einheitliches Referenzmodell bietet [39] und als Good Practice angesehen wird.[40]

Um die Qualität und Verfügbarkeit der IT-Services zu sichern, werden *Service Level Agreements* (SLA) zwischen den Partnern vereinbart und näher spezifiziert (Leistung und Ausprägung[41] sowie die Qualität der Services[42], die zu erbringen sind).

Ein SLA ist eine vertragliche und kennzahlenbasierte Vereinbarung zwischen zwei Parteien, dem Serviceanbieter und dem Kunden, in der Umfang und Güte der IT-Dienstleistung (IT-Services) beschrieben und die Vertragsbedingungen schriftlich fixiert werden.[43] Durch SLAs werden „die Qualitäten und Quantität der IT[-]Services zu vertretbaren Kosten verhandelt, definiert gemessen und kontinuierlich verbessert.“[44]

Die SLAs müssen in einem ganzheitlichen Rahmen eingebunden werden, d. h. dass sowohl der Anwender als auch das Management mit in den Prozess einbezogen werden muss, damit die SLAs ihre Wirkung entfalten können. Die einzelnen Inhalte der SLAs sollten neben technischen Aspekten auch die Serviceprozesse und die Servicequalität wiedergeben, da diese für die Servicenehmer von besonderer Bedeutung sind.[45]

Für die Anwendung der SLAs in der IT-Sicherheit bedarf es für den jeweiligen IT-Service eines oder mehrerer spezifischer Parameter, die es zu berücksichtigen gilt. Anhand der folgenden Tabelle werden exemplarisch wichtige Leistungsparameter der IT-Sicherheit, wie sie zu einer qualitativen Spezifizierung in SLA verwendet werden, gezeigt. Letztlich sollen die Parameter aufeinander abgestimmt und begründbar sein.[46]

---

[33] Vgl. Kopperger et. al (2007), S. 122.
[34] Kopperger et. al (2007), S. 12.
[35] Lehner et. al (2007), S. 223.
[36] Vgl. Lehner et. al (2007), S. 223f.
[37] Vgl. Prottung (2008), S. 71.
[38] Vgl. Lehner et. al (2007), S. 224.
[39] Vgl. Kopperger et. al (2007), S. 125.
[40] Vgl. Bon, von (2008), S. 21.
[41] Vgl. Hofmann (2007), S, 105.
[42] Vgl. Köhler et al. (2003), S. 348.
[43] Vgl. ebenda.
[44] Ebel (2008), S. 218.
[45] Vgl. Köhler et al. (2003), S. 348f.
[46] Vgl. Gründer (2007), S. 246.

Tabelle 2: Beispielhafte SLA-Parameter für Security Services[47]

SLA-Serviceparameter	Leistungsmerkmale
Verfügbarkeit	z. B.: 99,9% im Kalendermonat
Betriebszeit	i. d. R. 24 x7 x 52
Erreichbarkeit	i. d. R. 24 x7 x 52
Reaktionszeit	z. B.: maximal 5 Minuten
Datendurchsatz	z. B.: mind. 10 TB je Kalendermonat
Lösungszeit	z. B.: maximal 2 Kalendertage

Sollten IT-Security-Services fremd, also an einen externen Dienstleister, vergeben werden, so ist ein besonders gewissenhaftes Vorgehen bei der Erstellung der SLAs erforderlich, denn ein reibungsloser Ablauf des operativen Geschäfts muss gewährleistet sein.

3 Bedrohungen der Informationssicherheit und Investitionen in Schutzmaßnahmen

3.1 IT-Abhängigkeiten

Dem Gesetzgeber[48], den Unternehmen und Behörden ist die Abhängigkeit von der IT ebenso bewusst[49], wie die damit zusammenhängenden Sicherheitsbedrohungen.[50] Die Abhängigkeit der Geschäftsprozesse von der IT bei gleichzeitiger Zunahme der Komplexität der IT-Systeme zeigt, dass der Einsatz von Informationssicherheit notwendig ist.[51]
Viele Geschäftsprozesse hängen von einem reibungslosen Ablauf der IT und von der Qualifikation des Personals ab. Fällt nun die IT aus, muss schnell dafür gesorgt werden, dass das System wieder instand gesetzt wird. Die Abhängigkeit von der Informationstechnologie kann dazu führen, dass durch bestimmte fehlerhafte Prozesse das Image der Unternehmung auf Grund von Qualitätsproblemen, Lieferschwierigkeiten oder sonstigen Ursachen geschädigt wird. Falls die IT ausfällt und die Geschäftsprozesse nicht mehr ausführbar sind, kann dies sogar zur Insolvenz einer Unternehmung führen.

Diese Schäden müssen nicht zwangsläufig nur von der IT abhängen, sondern auch vom bedienenden Personal, das falsche Daten und Informationen bewusst oder unbewusst in das System eingibt oder falsche Daten durch Hacker eingeschleust oder die IT sabotiert wird. Durch das Supply Chain Management wird „die Betrachtung auf alle beteiligten Partner einer Wertschöpfung ausgedehnt, also z.B. auch auf Lieferanten, Logistikunternehmen und verschiedene Dienstleistungsanbieter.“[52] Dabei bestehen zwischen den Unternehmen meist Vernetzungen und Abhängigkeiten. Treffen Daten von Abnehmern falsch oder nicht vollständig bei den Zulieferern ein, kann es zu schwerwiegenden Produktionsausfällen kommen, die Hersteller, Lieferanten und natürlich den Kunden betreffen.

[47] Eigene Darstellung in Anlehnung an Gründer (2007), S. 247 nach gründer consulting (2006).
[48] Vgl. Schreiber (2006), S. 86.
[49] Vgl. Swoboda et al. (2008), S. IX.
[50] Vgl. Reichenbach (2004), S. 331.
[51] Vgl. Tsintsifa (2005), S. 219.
[52] Stahlknecht/Hasenkamp (2005), S. 365

Tabelle 3: Klassifikationsschema für IT-Abhängigkeit[53]

Bedeutung	Beschreibung
unterstützend	Bei IT-Ausfall ist die Fachaufgabe bei geringem Mehraufwand mit anderen Mitteln (z. B. manuell) zu erfüllen. Der Ausfall des Verfahrens ist auch für einen langen Zeitraum tolerierbar.
wichtig	Die Fachaufgabe ist nur mit deutlichem Mehraufwand und anderen Mitteln zu erfüllen. Der Ausfall des Verfahrens ist längere Zeit tolerierbar.
wesentlich	Die Menge der anfallenden Vorgänge/Informationen lässt lediglich ein fragmentarisches Erfüllen der Fachaufgabe mit den verfügbaren Ressourcen zu. Der Ausfall des Verfahrens ist nur für eine begrenzte Zeit tolerierbar.
hochgradig notwendig	Die Fachaufgabe kann ohne IT-Einsatz nicht durchgeführt werden. Kritische Applikationen können nicht durch manuelle Verfahren ersetzt werden. Die Ausfalltoleranz ist auf Grund des Schadenspotentials sehr gering.

Da die IT Risiken unterliegt, externe oder interne Bedrohungen, ist die Abhängigkeit groß. Auf Grund der überragenden Bedeutung der Funktionsfähigkeit der IT sollten geeignete Schutzmaßnahmen ergriffen werden, um den Bedrohungen angemessen zu begegnen.[54] „Eine Bedrohung (engl. *threat*) des Systems zielt darauf ab, Schwachstellen oder Verwundbarkeit auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen, oder um die Authentizität von Subjekten zu gefährden."[55]
Da die Computer zunehmend miteinander vernetzt sind, die Geschäftsprozesse auch ins Internet verlagert werden und die Komplexität der IT stetig zunimmt, erhöht sich die Gefahr von Angriffen. Eines direkten Zugangs zu den Systemen bedarf es heute nicht mehr, denn viele Angriffe werden über das Internet initialisiert, so dass sich die Chance einer direkten Zuordnung zum Täter verringert.[56]

Tabelle 4: Gefährdungsursachen[57]

menschlichen Ursachen	Fehlbedienungen des Systems auf Grund von Benutzungsfehlern durch mangelnde Ausbildung oder Erfahrung, Überlastung der Nutzer, mangelnde Benutzerfreundlichkeit oder zu weit reichende Zugriffsrechte. Der Ausfall von Informationsträgern durch mangelnde Wartung oder Bedienung oder gar die Nichtbenutzbarkeit von Systemen auf Grund von Fehlzeiten, Urlaub, Kündigung, oder Versetzung. Ebenso gelten Angriffe auf das System als menschliche Ursachen, auf Grund von Bereicherung oder um Schaden herbeizuführen, welche durch Sabotage, Diebstahl, Spionage, Betrug oder ungewollt im Scherz begangen werden.
technischen Ursachen	Mängel an der Hardware verursacht durch fehlende Wartung, falsche Installation und Konfiguration sowie Überlastung, die zu Fehlfunktionen, Leistungsabfällen oder gar zu einem kompletten Systemversagen führen können. Daneben kann die Software Systemabstürze und Fehler durch einen Programmfehler, falsche Konfiguration oder Inkompatibilität mit anderen Programmen bedingen.
Umweltbedingte Ursachen	Unfälle und Katastrophen (Feuer, Wasser, Erdbeben, Stürme) und Kriege sowie lokale Unruhen, die die Systeme beschädigen oder eventuell komplett vernichten können. Menschliche Ursachen stellen die häufigsten Bedrohungen dar, dabei sind es keine vorsätzlichen Handlungen sondern die Bedrohung entsteht auf Grund fehlenden Wissens, Leichtfertigkeit oder falscher Einschätzung der Umgebung.[58]

[53] Eigene Darstellung in Anlehnung Wiedemann (2007), S. 21.
[54] Vgl. Lassmann (2006), S. 349f.
[55] Eckert (2008), S. 15 (Hervorhebung im Original).
[56] Vgl. Lassmann (2006), S. 349f.
[57] Vgl. im Folgenden Lassmann (2006), S. 350f.
[58] Vgl. Wiltner (2003), S. 82.

Die gefährdeten Objekte sind in der Folgenden Tabelle aufgeführt.

Tabelle 5: Gefährdete Objekte[59]

Hardware	Ausfall ganzer Systeme oder einzelner Bereich von Datenträgern, Rechnern, externen Geräten und Kommunikationsnetzen
Software	Programm- und Systemabstürze, Fehlfunktionen, Löschen oder Ändern von Software, unbefugtes Ausführen von Programmen, Erstellung von Raubkopien, Infektion mit Computerviren
Daten	Unbefugtes Erzeugen, Lesen, Ändern, Löschen oder Kopieren
Kommunikation	Benutzung einer falschen Identität, Abhören von übertragenen Daten, Verändern von übertragenen Daten, Wiederholung einer Übertragung zu einem späteren Zeitpunkt, Leugnen der Kommunikation, Verhindern oder Unterbrechen der Kommunikation, Analyse der Häufigkeit der Kommunikation, unbefugtes Eindringen in entfernte Systeme
Organisation	zu weit gehende Zugangsberechtigungen, fehlender Zugang zu Informationen oder Teilen des Systems, erschwerte Erweiterung oder Wartung des Systems

Die nachstehende Abbildung 1 zeigt den Zusammenhang zwischen den Gefahren und den Objekten der Gefährdung auf.

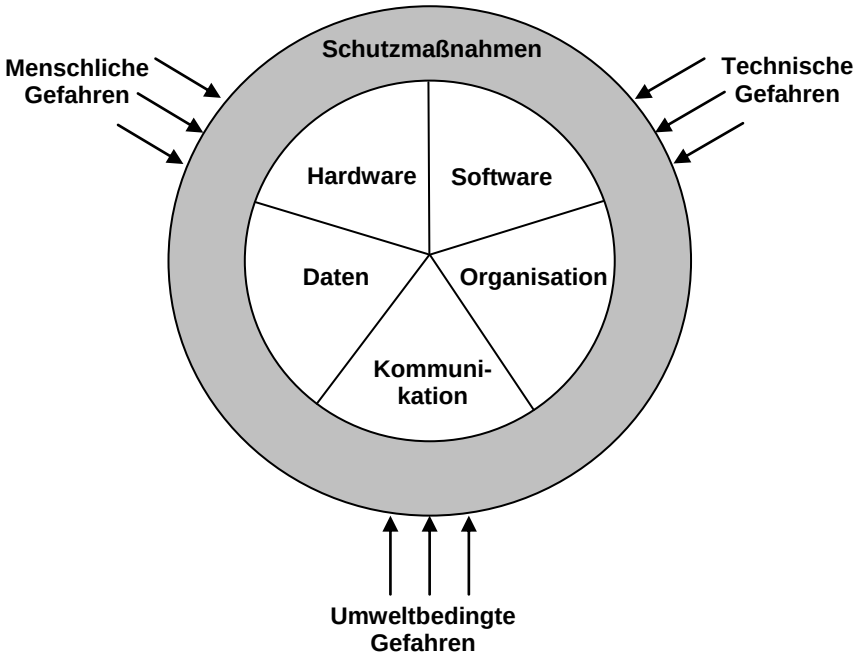


Abbildung 1: Gefahrenpotentiale der IT
Quelle: eigene Darstellung in Anlehnung an Lassmann (2006), S. 349

Die folgenden Studien sehen die Menschen in einer Organisation als die größte Gefahr.

[59] Lassmann (2006), S. 351.

Tabelle 6: kes - Bedeutung der verschiedenen Gefahrenbereiche[60]

	Vorhersage 2006		Bedeutung heute		aktuelle Prognose		Schäden	
	Rang	Priori-tät	Rang	Prio-rität	Rang	Prio-rität	Rang	ja, bei
Malware (Viren, Würmer, Trojanische Pferde, ...)	1	1,51	1	1,12	1	1,29	4	21%
Irrtum und Nachlässigkeit eigener Mitarbeiter	2	1,17	2	0,93	2	0,79	1	36%
Hacking (Vandalismus, Pro-bing, Missbrauch, ...)	4	0,59	3	0,58	3	0,77	8	11%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirt-schaftsspionage	3	0,63	4	0,55	4	0,71	7	12%
Software-Mängel/Defekte	5	0,58	5	0,54	5	0,49	3	26%
Hardware-Mängel/Defekte	6	0,34	6	0,45	9	0,28	2	34%
Mängel der Dokumentation	9	0,27	7	0,40	10	0,27	6	15%
unbeabsichtigte Fehler von Externen	7	0,32	8	0,36	8	0,34	5	16%
Sabotage (inkl. DoS)	10	0,22	9	0,36	6	0,46	10	6%
Manipulation zum Zweck der Bereicherung	8	0,29	10	0,34	7	0,38	9	8%
höhere Gewalt (Feuer, Wasser, ...)	11	0,03	11	0,25	11	0,15	11	4%
Sonstiges	12	0	12	0,06	12	0,01	12	2%

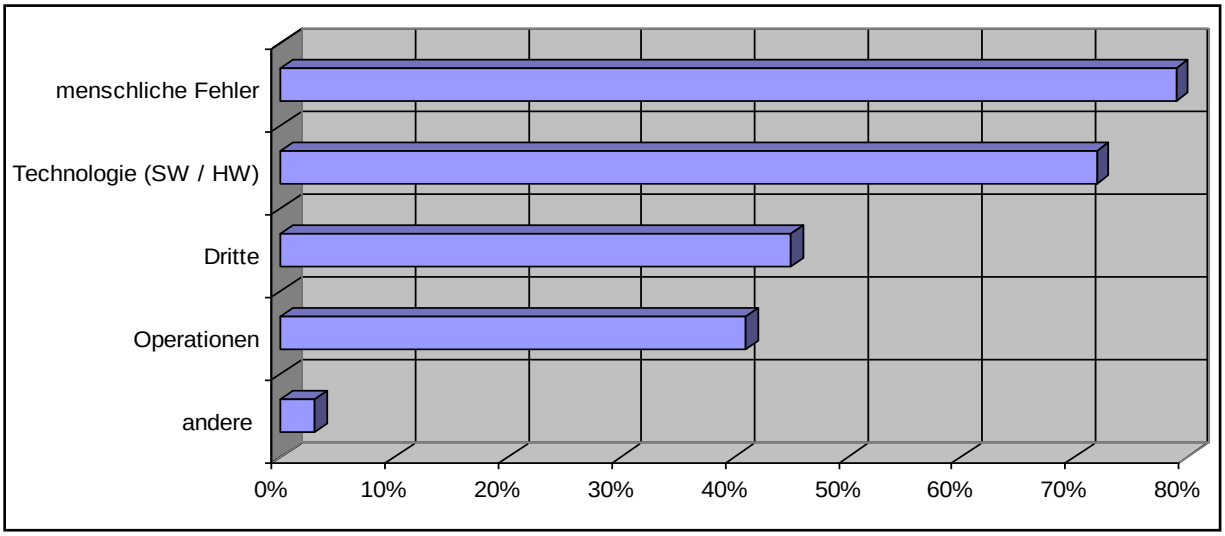


Abbildung 2: Gefahrenursachen der IT-Fehler[61]

Daher müssen geeignete Schutzmaßnahmen von den Unternehmen ergriffen werden, um sich vor den Bedrohungen und Gefahren zu schützen.

[60] Eigene Darstellung in Anlehnung an Lagebericht zur Informations-Sicherheit 1, o.V. (2008), kes 2008#4, S. 3.
[61] Eigene Darstellung in Anlehnung an Deloitte (2007), S. 25.

3.2 Bedrohungen und Schaden

Unter dem Begriff *externe Bedrohungen* werden Bedrohungen subsumiert, die von außen auf eine Unternehmung oder Behörde einwirken und ihr dadurch Schaden zufügen. Dieser Schaden kann finanzieller Natur sein oder eine Lähmung des Systems darstellen.
Die größte Bedrohung sehen die Firmen nicht mehr in den Menschen selbst, wie es in den vergangenen Jahren der Fall war, sondern in Malware, d. h. in Viren, Würmern und Trojanischen Pferden, welche meist von außen in das IT-System eingeschleust werden. Weitere Bedrohungen gehen von Hackern und Crackern aus
Interne Bedrohungen sind Gefahren für eine Unternehmung oder eine Behörde, die von innen aus der Unternehmung/Behörde heraus durch deren Mitarbeiter oder Dritte, die sich unberechtigt Zugang beschafft haben (siehe Social Engineering), entstehen.
Zu dieser Art von Bedrohung zählen Datendiebstähle, Sabotage, Fahrlässigkeit der Mitarbeiter und Betrug.[62]

Für die angesprochenen Risiken bzw. Bedrohungen müssen die jeweiligen Eintrittswahrscheinlichkeiten und Schadenshöhen ermittelt werden. „Ein Schaden ist definiert als Nachteil, der durch Minderung oder Verlust von Vermögen entsteht. Schäden können materieller, aber auch immaterieller bzw. ideeller Natur sein.“[63] Die Schadenshöhe ist eine Zusammensetzung aus bezifferbarem und nicht direkt bezifferbarem Schaden[64], der monetär bewertet wird.[65] wobei die Risikohöhe den bezifferbaren Schaden bei Eintritt des Risikos angibt.[66]
Die Eintrittswahrscheinlichkeit gibt die Wahrscheinlichkeit an, dass ein Risiko eintritt.[67] Die Risikohöhe und die Eintrittswahrscheinlichkeit können anhand von unterschiedlichen Maßnahmen identifiziert werden. Nach der Formel:*„Schadensausmaß = Eintrittswahrscheinlichkeit * Risikohöhe“*[68] lässt sich das Schadensausmaß für jede einzelne Bedrohung (Risiko) berechnen und in einer Risikomatrix abgetragen werden. Drei Bereiche sind zu unterscheiden: der Akzeptanzbereich, der kritische Bereich und der Gefahrenbereich (vgl. Abb. 3).[69]
Im Umgang mit Risiken existieren unterschiedliche Vorgehensweisen, wie mit dem identifizierten Risiko verfahren werden kann: Im Akzeptanzbereich sollte das Risiko akzeptiert werden, da die Schadenshöhen und Wahrscheinlichkeiten relativ gering sind. Bei größeren Risiken sind diese an Dritte auszulagern - hier kommt z. B. eine Versicherung zum Tragen (bei niedriger Eintrittswahrscheinlichkeit und hohem finanziellen Schaden) - oder ob die Risiken durch bestimmte Maßnahmen wie z. B. Awareness Programme (bei Mitarbeiterrisiken) minimiert oder gar vermieden werden können. Ist eine Vermeidung oder Verminderung der Risiken nicht möglich (Gefahrenbereich), sollten entsprechende Gegenmaßnahmen geplant werden, die zum Einsatz kommen, um dem Risiko zu begegnen.[70]

[62] Vgl. Dolya (2007a), S. 5.
[63] Hoppe/Prieß (2003), S. 28.
[64] Vgl. Seibold (2006), S. 13.
[65] Vgl. Hoppe/Prieß (2003), S. 29.
[66] Vgl. Ahrendts/Morton (2008), S. 23.
[67] Vgl. Seibold (2006), S 21.
[68] Ahrendts/Morton (2008), S. 23.
[69] Vgl. Ahrendts/Marton, S. 25.
[70] Vgl. Ahrendts/Marton, S. 29.

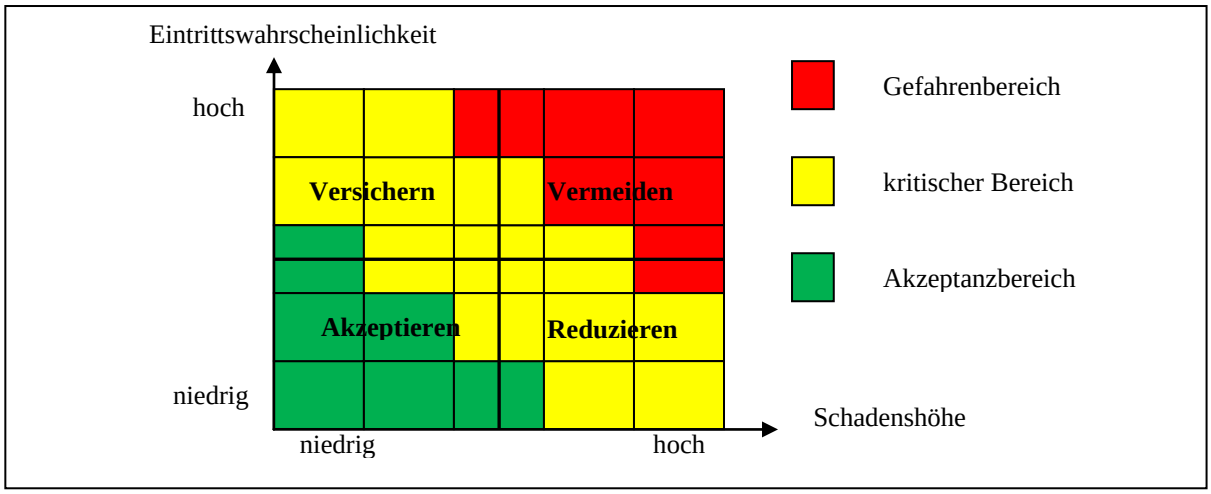


Abbildung 3: Risikomatrix[71]

Um die Risiken zu minimieren oder andere entsprechende Vorgehensweisen zu implementieren, muss die IT-Sicherheit dementsprechend aufgestellt sein und ihr müssen die nötigen Ressourcen, wie finanzielle aber auch personelle Mittel, zur Verfügung stehen. Die Investition in die IT-Sicherheit wird nun näher betrachtet.

3.3 „Value of IT“: die Investitionen in die Informationssicherheit

Alle Anwendungen, Netze, Systeme, Infrastrukturen und Informationen verfügen über einen Bedarf an Sicherheit, der als *Schutzbedarf* bezeichnet wird. Bei der Schutzbedarfsanalyse gilt es, die entstehenden Schäden der einzelnen Systeme zu ermitteln, wenn die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität nicht mehr gewährleistet werden können.[72]

Tabelle 7: Schutzbedarfsklassen nach dem Grundschutzhandbuch des BSI[73]

Normal bis mittel	Eine Auswirkung des Schadens ist überschaubar und begrenzt, d. h. der eintretende finanzielle Schaden ist hinnehmbar und die Geschäftsprozesse werden, wenn überhaupt, nur peripher tangiert.
Hoch	Die Schadensauswirkungen können beträchtlich sein, dies bedeutet eine Spürbarkeit des finanziellen Schadens und eine Beeinträchtigung der Geschäftsprozesse sowie eine Drohung von signifikanten Ausfallzeiten.
Sehr hoch	Die Schadensauswirkungen können ein katastrophales, existentiell bedrohliches Ausmaß annehmen, d. h. der finanzielle Schaden bedroht die Existenz der Unternehmung und/oder der Geschäftsprozessausfall kann zu Imageschäden oder dem Verlust von Aufträgen führen.

Ziel nach der Ermittlung der Schutzbedarfe ist es, mittels geeigneter Anwendung von personellen, technischen sowie physikalischen und prozessualen Schutzmaßnahmen[74] ein adäquates Sicherheitsniveau zu erreichen.[75] Die auszuwählenden Schutzmaßnahmen sollten der Unternehmung und den zu schützenden Komponenten angepasst sein, d. h. die Kosten für die Sicherheitsmaßnahmen sollten dem Schutzobjekt entsprechen.

[71] Eigene Darstellung in Anlehnung an Ahrendts/Marton (2008), S. 26; Geiger (2007), S. 45.
[72] Vgl. Humpert (2004), S. 10 sowie Friberg et al. (2003), S. 69.
[73] Vgl. im Folgenden Eckert (2008), S. 167; Hofmann (2007a), S. 255; Friberg et al., S. 69.
[74] Synonym für den Begriff Schutzmaßnahme wird in der Literatur der Begriff Sicherheitsmaßnahme verwendet.
[75] Vgl. Friberg et al. (2003), S. 70.

Die Investition in IT-Schutzmaßnahmen ist eine Zukunftsinvestition. Es ist bereits bei der Planung auf das Kosten-Nutzen-Verhältnis zu achten,[76] da sich die IT- sowie Informationssicherheit der Gewinnmaximierung von Unternehmen unterordnet.[77]
Ziel ist es, *wirtschaftliche Schutzmaßnahmen* einzusetzen, die dem Unternehmen ein hohes Sicherheitsniveau zu geringen Kosten offerieren. Es ist eine Optimierung der Maßnahmen anzustreben. Dies „bedeutet, dass die Summe aus den Kosten für Sicherheitsmaßnahmen und dem durch Sicherheitsmängel entstehenden Schaden minimiert wird.“[78] Hervorzuheben ist, „dass die Risikominimierung nicht linear mit dem Investment steigt.“[79] Der größte Schutzeffekt wird meist durch die erste Investition in die IT-Sicherheit erzielt. Weitere Investitionen erhöhen das Sicherheitsniveau, die Kosten steigen jedoch exponentiell an. Pohlmann folgert:[80]

1. Das Pareto-Prinzip gilt auch für die IT-Sicherheit, d. h. setzt man 20% der möglichen IT-Schutzmaßnahmen richtig ein, dann kann ein 80%-iger Schutz vor Bedrohungen realisiert werden.
2. Ist bereits ein Grundschutz implementiert, werden weitere Investitionen in die Sicherheit sehr hoch sein und somit wirtschaftlich nicht sinnvoll, jedoch kann es notwendig sein, in die Sicherheit zu investieren, z. B. auf Grund neuer Gesetze, neuer Technologien, zum Schutze der Gesellschaft oder weil mit kostengünstigen Verfahren doch noch das Sicherheitsniveau erhöht werden kann (z. B. Awareness Kampagnen, Mitarbeitersensibilisierung und -schulungen).

Vielfach werden die Entscheidungen über die Schutzmaßnahmen nicht von Sicherheitsexperten gefällt, sondern vom Management. So wird häufig ein Punkt rechts oder links neben dem Optimum (welches in Abbildung 4 der dicke Punkt der Kurve für das optimale Kosten-Nutzen-Verhältnis symbolisiert) realisiert, da Entscheider und Entscheidungsvorbereiter in Ihren Bewertungen bzgl. des Sicherheitsniveaus und der dafür benötigten Schutzmaßnahmen nicht übereinstimmen. Um wirtschaftlich zu agieren, sollte ein Punkt in der Nähe des Optimums gewählt werden.[81]

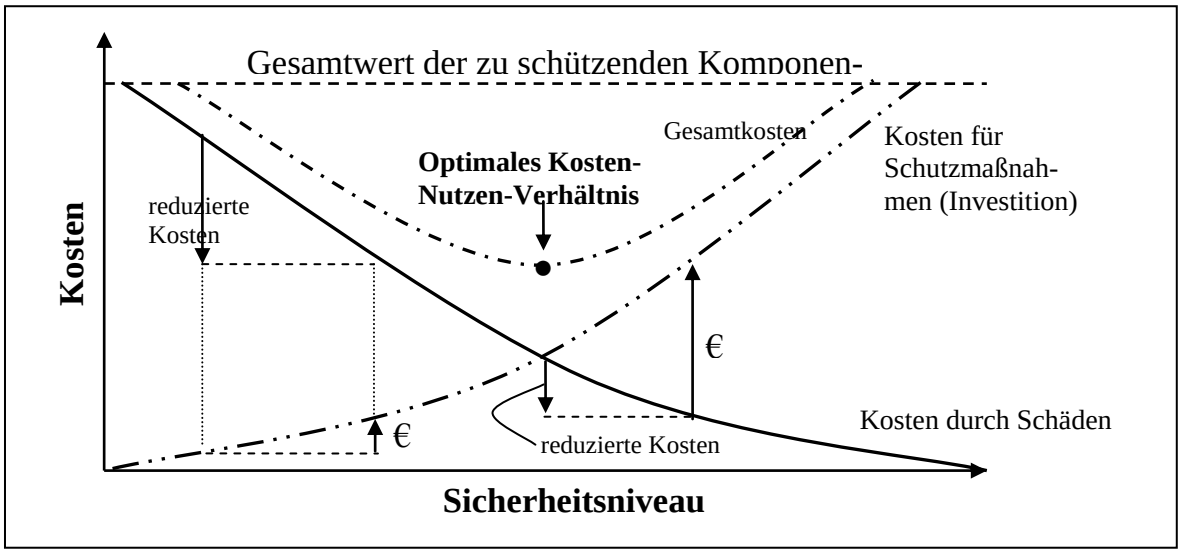


Abbildung 4: Kosten-Nutzen-Verhältnis von Schutzmaßnahmen[82]

[76] Vgl. Pohlmann/Blumberg (2006), S. 457.
[77] Vgl. Schreiber (2006), S. 86.
[78] Schreiber (2006), S. 86.
[79] Pohlmann (2006), S. 28.
[80] Vgl. im Folgenden Pohlmann (2006), S. 28f.
[81] Vgl. ebenda, S. 278f.
[82] Eigene Darstellung in Anlehnung an Raepple (2001), S. 9 und Pohlmann (2004), S. 29.

Mit Hilfe des *Return on Security Investment* (RoSI) kann der Nutzenaspekt der Schutzmaßnahmen berechnet werden[83] (vgl. Abb. 5).

„RoSI bedeutet, dass bei der Betrachtung aller Kosten (auch die, die durch Schäden eines Angriffes verursacht werden) aufgezeigt werden kann, ob und wann ein Investment in IT-Sicherheitsmaßnahmen zu einem Return on Investment führt oder nicht.“[84]

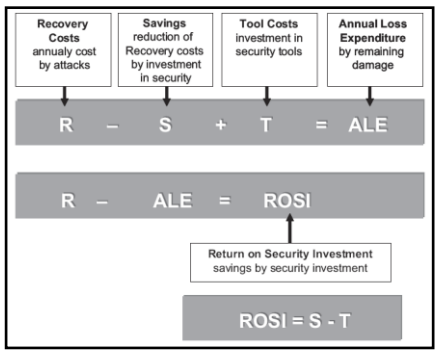


Abbildung 5: Berechnung des RoSI
Quelle: Pohlmann (2006), S. 30

Recovery Costs (R) sind die Kosten der wahrscheinlichen Schäden, hierzu zählen alle Aufwendungen, die nötig sind, um nach einem eingetretenen Schaden den Urzustand zu rekonstruieren. Die Recovery-Kosten müssen aus den zukünftigen Erwartungswerten geschätzt werden, obgleich sie vom tatsächlichen Eintritt der Schäden abhängen. *Savings* (S) bezeichnen die reduzierten Kosten der wahrscheinlichen Schäden, die durch den Einsatz von Schutzmaßnahmen eingespart werden, da diese einen Angriff mit großer Wahrscheinlichkeit abwehren. *Tool Costs* (T) sind die Kosten für die Schutzmaßnahmen. *Annual Loss Expenture* (ALE) beziffert die verbleibenden Kosten bzw. den Schaden nach einer Investition in IT-Schutzmaßnahmen. *RoSI* sind letztlich die gesparten Kosten bzw. nicht eingetretene Schäden auf Grund des Einsatzes von Schutzmaßnahmen. Solange die Tool Costs kleiner als die Savings sind, ist der RoSI positiv.
Der RoSI kann mittel der Formel: $R – (R – S – T) = RoSI = S – T$[85] berechnet werden.

Problematisch beim Return on Security ist jedoch, dass unterschiedliche Risiken gleich behandelt werden: zum einen Risiken mit hoher Eintrittswahrscheinlichkeit und geringem Schadensausmaß und zum anderen Risiken mit geringer Eintrittswahrscheinlichkeit und hohem Schadensausmaß. Des Weiteren muss die Ersparnis, die aus der Schutzmaßnahme resultiert, geschätzt werden und liefert damit keine zuverlässigen Daten. Außerdem ist wenig über die tatsächlichen bzw. zu erwartenden Häufigkeiten von Schäden bekannt, die allerdings für die Berechnung des Risikos benötigt werden.[86]
Die Schäden müssen nicht nur qualifiziert sondern auch quantifiziert werden, um den RoSI zu berechnen und in der Praxis nutzbar zu machen, daher müssen Bedrohungen und deren Schäden dokumentiert werden, damit die tatsächlichen Kosten ermittelt werden können.[87]

Eine Unternehmung hat eine Vielzahl von Systemen, Software, Netzwerken und Akteuren, die in ein Sicherheitskonzept eingebunden werden müssen. Diese Komponenten und Akteure sowie zwei Menschenbild Typologien werden im folgenden Kapitel näher beschrieben.

[83] Vgl. Pohlmann (2006), S. 29.
[84] Pohlmann (2006), S. 29.
[85] Vgl. Pohlmann (2006), S. 29f.
[86] Vgl. Schadt (2006), S, 21.
[87] Vgl. Pohlmann (2006), S. 34.

4 Komponenten und Akteure in der Informationssicherheit

4.1 Hard- und Softwarekomponenten

Hardware bezeichnet alle physikalischen Einheiten, die genutzt werden, um ein Rechnersystem aufzubauen. Die Clients und Server sind über Netzwerke miteinander verbunden, um einen Datenaustausch zu ermöglichen. Des Weiteren werden Notebooks, Personal Digital Assisstants (PDA) und zunehmend auch Smartphones in die Firmennetzwerke eingebunden, um auch hier einen Datenabgleich zu ermöglichen.[88]
Um die Daten und Informationen innerhalb eines Netzwerkes zu schützen, lassen sich *Firewalls* installieren. „Eine Firewall ist ein Sicherungssystem, das das Eindringen von Benutzern externer Netze, insbesondere des Internets, in Unternehmensnetze verhindern soll."[89] Die Firewall schottet daher Netze durch Kontrollen und Filter voneinander ab und verhindert eine Weitergabe von Datenpaketen, die eine Bedrohung für das System darstellen.

Mittels *Software*[90] lässt sich die Hardware schützen. Softwarekomponenten lassen sich in drei Unterarten gliedern: Systemsoftware, Anwendungssoftware und Unterstützungssoftware.
Die Systemsoftware dient der Steuerung des Computers, ihr zentraler Bestandteil ist das Betriebssystem.[91] Die Anwendungssoftware erbringt eine spezifische Leistung, um den Computer für die vielfältigsten Aufgabengebiete nutzen zu können.[92] Die Unterstützungssoftware „ist für spezielle Aufgaben bei der Softwareentwicklung und -wartung sowie beim Einsatz von anderer Software zuständig."[93] Für diese Arbeit relevante systemnahe Software sind Virenschutzprogramme und personal Firewalls.

Tabelle 8: Relevante, systemnahe Software

Virenschutzprogramme	Virenschutzprogramme werden eingesetzt, um Schäden durch Computerviren, Würmer und Trojanische Pferde abzuwehren, wobei sie permanent im Hintergrund laufen und jede neue Datei auf eine Infizierung prüfen. Auch Virenschutzprogramme können auf Grund von eigenen Sicherheitslücken zu einem Sicherheitsproblem avancieren.
Personal Firewalls	Personal Firewalls schützen ein einzelnes System, jedoch kein komplettes Unternehmensnetzwerk. Sie sind primär für die Verwendung bei internetgebundenen Arbeitsplatzrechnern vorgesehen. Die Firewall regelt den Zugang auf und vom Rechner über freigegebene Adressen und Ports, damit Anwender wissen, welche Programme auf das Internet zugreifen oder welche Daten aus dem Internet empfangen werden. Die Konfiguration erfolgt über Paketfilter, welcher mittels eines Regelwerkes entscheidet, ob Datenpakete empfangen oder blockiert werden. Eine personal Firewall zielt darauf ab, konzeptionelle Lücken wie back doors, Malware-Attacken auf Datenebene oder interne Attacken zu schließen, die bei einer zentralen Hardware-Firewalls und Virenschutzprogrammen noch vorhanden sein können.

[88] Vgl. Mertens et al. (2005), S. 14.
[89] Stahlknecht/Hasenkamp (2005), S. 494.
[90] Vgl. Rotenstrauch/Schulze (2003), S. 54.
[91] Vgl. Holey et al. (2004), S. 32.
[92] Vgl. Holey et al. (2004), S. 33.
[93] Stahlknecht/Hasenkamp (2005), S. 67.

4.2 Akteure der Informationssicherheit

Strategische Entscheider sind Mitarbeiter der Geschäftsleitung, Informationsmanager (CIO), Sicherheitsmanager aber auch Sicherheitsexperten der IT-Abteilungen. Die Entscheider sollten eine Vorbildfunktion haben. Das Management ist für die gesamte Unternehmung verantwortlich, somit auch für die Informationssicherheit. Ihnen obliegt die Garantie der Informationssicherheit durch die Umsetzung geeigneter Maßnahmen.[94] Bedeutsam ist, dass die erforderlichen Ressourcen bereitgestellt werden. An erster Stelle stehen die monetären Mittel, die benötigt werden, um den Schutz durch technische Maßnahmen zu realisieren, aber auch organisatorische, konzeptionelle und insbesondere personelle Maßnahmen sind zu ergreifen.[95] Zu letzteren gehören Schulungen und die Sensibilisierungen der Mitarbeiter.[96]
Problematisch ist, dass es an Unterstützung und dem Bewusstsein für Sicherheit seitens des Top- und mittleren Managements fehlt; 55% des Topmanagements treiben die Sicherheit nicht voran und sehen diese als lästiges Übel und bei 45% des mittleren Managements fehlt das Bewusstsein für die Sicherheit und deren Konsequenzen.[97]

Die *Administratoren* verfügen auf Grund ihrer Tätigkeit über weit reichende Kompetenzen, die sie dafür nutzen können, um die Systeme sicher in Betrieb zu halten.[98] Administratoren können ihre Kompetenzen jedoch auch ausnutzen. Missbräuche wie Datendiebstähle oder Manipulationen bleiben vielfach sehr lange unentdeckt.[99] Auch die Administratoren haben eine Vorbildfunktion; durch Schulungen immer wieder auf den neuesten Wissensstand gebracht,[100] sollten sie die IT-Sicherheitsrichtlinien nicht nur Verinnerlicht haben, sondern diese auch in die Praxis umsetzen können.
Wenn Administratoren ihren Aufgaben (z. B. die Prüfung von Backups und den Backupgeräten selbst) nicht nachkommen, kann es geschehen, dass die Daten nicht mehr ordnungsgemäß wiederhergestellt werden können oder sie überhaupt nicht mehr verfügbar sind, da entweder die Backups beschädigt sind oder gar das Backupgerät defekt ist.

Neben den Administratoren sorgen auch die *Softwareentwickler* für Bedrohungen. In diversen Programmen und Betriebssystemen sind Hintertüren (engl. back doors) eingebaut, die von den Entwicklern zu Testzwecken und zur Einspeisen neuer Softwareversionen verwendet werden. Diese Hintertüren bieten Unbefugten die Möglichkeit, auf die gespeicherten Daten und Informationen zuzugreifen, um eine Unternehmung gezielt oder ungezielt zu schädigen.[101]
Eine weitere Bedrohung geht von Hard- und Softwarefehlern aus, die durch ein mangelhaftes System-Design ausgelöst werden können. Ist die Qualifikation der Entwickler nicht ausreichend, entstehen Sicherheitsrisiken, z. B. der Ausfall der Soft- und/oder Hardware.[102]
Insgesamt werden in einer Unternehmung 60% aller Sicherheitslücken durch die eigenen Mitarbeiter (Insider)[103], dies schließt die Geschäftsleitung, Administratoren, IT-Spezialisten und

[94] Vgl. Schwyter/Wisler (2007), S. 7.
[95] Vgl. Schlienger (2003), S. 34.
[96] Vgl. ebenda.
[97] Vgl. ohne Verfasser (2008a), S. 8 kes Lagebericht zur Informations-Sicherheit (2) (2008).
[98] Vgl. BSI (2007), S. 15.
[99] Vgl. Wiltner (2003), S. 85.
[100] Vgl. Baier et al. (2003), S. 183.
[101] Vgl. Wiltner (2003), S. 85.
[102] Vgl. Gabriel (2006), S . 444 und Schadt (2006), S. 17.

Nutzer mit ein, verursacht. Das größte Schadenspotential jedoch geht von den *Nutzern* selbst aus, denn es fehlt 69% der Mitarbeiter an Sicherheitsbewusstsein.[104] Die Schäden resultieren dann aus unterschiedlichen Gründen:[105] Fehlendes Sicherheitsbewusstsein, Unkenntnis, Fehlbedienung von Hard- und Software und absichtliche Schädigung.

In einer durch die Firma known Sense durchgeführten Tiefenpsychologie Security-Studie, wurde herausgefunden, dass eine Versachlichung und Entmenschlichung der Arbeit stattfindet. Je weniger persönliche Dinge auf einem Computer zugelassen werden, desto höher ist die Gefahr eines Ausbruchs unsicherer Handlungen durch die Mitarbeiter, die sich in Fehlleistungen niederschlagen. Die Studie hält fest, dass innerhalb der Unternehmenskultur Raum für eben diese Ausbrüche gelassen und gegen diese gesteuert werden muss. Dabei helfen lebendige, gute und am besten unbewusste Awareness Kampagnen. Durch einen Mix an geeigneten Mitteln kann dann sowohl die Informations- und IT-Sicherheit, als auch die Motivation und Arbeitsleistung der Mitarbeiter gesteigert werden, indem gegen eine Versachlichung und gleichzeitigen Entmenschlichung der Arbeit vorgegangen wird.[106]
DVD-Laufwerke sowie USB-Schnittstellen können dazu beitragen, dass Viren, Würmer, Trojaner oder andere schädliche Programme in das Netzwerk bewusst oder fahrlässig eingeschleust werden.[107] Nicht nur das Einbringen von Schadprogrammen birgt Gefahren sondern auch die Möglichkeit, Daten zu kopieren und zu stehlen. Laut kes Studie 2008 hat die Gefährdung durch Datenträger stark zugenommen (vgl. Tab. XX).[108]

Tabelle 9: Infektionswege von Malware[109]

Infektionsquelle	häufig	selten	nie	Bedeutung*
E-Mail	46%	35%	19%	1,72
Internet-Download	34%	41%	24%	1,44
Webseiten (aktive Inhalte)	19%	43%	37%	1,01
Datenträger	16%	53%	31%	1,00
mobile Systeme	13%	49%	38%	0,89
Internet (autom.Verbreitung)	14%	41%	45%	0,83
unbekannte Herkunft	12%	40%	49%	0,75
internes Netz	8%	25%	67%	0,48

Jeder Mensch geht mit der Sicherheit der Daten, den Informationen und dem System sowie den möglichen Risiken unterschiedlich um, da Denkweisen, Kenntnisse und die Einstellung im Hinblick auf die Sicherheit differieren. Diese unterschiedlichen Einstellungen und Denkweisen können in unterschiedlichen Menschenbildern zusammengefasst werden, wovon im Folgenden zwei Menschenbildtypologien näher erläutert werden.

[103] Vgl. Schlienger (2003), S. 34.
[104] Vgl. ohne Verfasser (2008a), S. 8, kes Lagebericht zur Informations-Sicherheit (2) (2008).
[105] Vgl. hierzu und im Folgenden Temme (2004), S. 11.
[106] Vgl. hierzu Pokoyski (2006), S. 1f.
[107] Vgl. Uth et al. (2008), S. 40.
[108] Vgl. ohne Verfasser (2008), S. 6, kes Lagebericht zur Informations-Sicherheit (1) (2008).
[109] Lagebericht zur Informations-Sicherheit 1, ohne Verfasser (2008) kes 2008#4 S. 9.

4.3 Exkurs: Unterschiedliche Menschenbilder der Akteure

Modelle und Theorien in der BWL gehen explizit oder implizit von Vorstellungen über handelnde Individuen in Organisationen aus, kurz Menschenbild genannt. Ziel der idealtypischen Menschenbilder ist es, eine Komplexitätsreduktion der einzelnen Facetten der menschlichen Natur und der damit zusammenhängenden Ziele, Motive, Werte und Fähigkeiten zu ermöglichen.

Die Mitarbeiter eines Unternehmens können mittels des Konstrukts Menschenbilder bezüglich Ihrer Einstellungen und Motive zur Informationssicherheit analysiert und beeinflusst werden. Dies nutzen sowohl Managementtheoretiker als auch -praktiker gleichermaßen.[110] Der Begriff Menschenbild wird in der Literatur unterschiedlich definiert.[111]

Nach Weinert spiegelt es „…die Einstellung zur Natur eines Menschen wieder[…]. Es ist die Grundeinstellung dazu, ob der Mensch ehrlich, geradlinig und vertrauenswürdig ist, oder ob er dazu neigt, jeden Vorteil um jeden Preis zu nutzen.“[112] Bei Menschenbildern „handelt es sich um Grundannahmen, Einstellungen und Erwartungen von Führungskräften gegenüber den Zielen, Fähigkeiten, Motiven und Werten der Mitarbeiter.“[113]

Dualistisches Menschenbild nach McGregor

Donald McGregor[114] entwickelte das sehr eingängige, mitunter aber auch zu stark simplifizierte Konstrukt des dualistischen Menschenbildes.[115] McGregor geht von zwei diametralen gegenüberstehenden Menschenbildern aus, der Theorie X und der Theorie Y[116] und beschreibt deren Auswirkung auf das Führungsverhalten der Vorgesetzten.[117] Nach Annahme von McGregor beruht „jede Führungsentscheidung auf einer Reihe von Hypothesen über die menschliche Natur und menschliches Verhalten.“[118] In der Theorie X verarbeitet er die Annahmen des rational-ökonomischen Menschenbildes[119], also alle Annahmen der traditionellen Managementansätze, und stellt der Theorie X die idealtypische Theorie Y gegenüber.[120]

Die Theorie X beschreibt den Menschen als ein träges und inaktives Wesen,[121] welches faul und verantwortungsscheu ist und zur Arbeit durch die Vorgesetzten angetrieben, angehalten und motiviert werden muss.[122] Um den Menschen zur Arbeit zu bewegen, muss dieser streng kontrolliert und beaufsichtigt werden; es handelt sich dementsprechend um eine Führung durch Lenkung und Kontrolle mittels Autorität[123] (autoritärer Führungsstil)[124].

---

[110] Vgl. Staehle (199), S. 432.
[111] Vgl. Blickle (2004), Sp. 836f ; Staehle (1999), S. 432; Weinert (2004), S. 664.
[112] Weinert (2004), S. 87.
[113] Weinert (2004), S. 664.
[114] Douglas McGregor (1906-1964) war Professor für Management am Massachusetts Institute of Technology.
[115] Vgl. Steinle/Ahlers (2004), Sp. 1145.
[116] Vgl. Steinle (1978), S. 190.
[117] Vgl. Jung (2006), S. 395.
[118] Staehle (1999), S. 192.
[119] Vgl. Hesch (1997), S. 92.
[120] Vgl. Stahle (1999), S. 192.
[121] Vgl. Weinert (1995), Sp. 1499.
[122] Vgl. Neuberger (2006), S. 345f.
[123] Vgl. Hesch (1997), S. 95.
[124] Vgl. Töpfer (2005), S. 946.

Die Theorie Y dagegen basiert auf Maslows Bedürfnispyramide[125] und hat wie sie die Selbstverwirklichung zum Ziel.[126] Sie beschreibt den Menschen als ein sich entwickelndes Wesen,[127] welches kreativ ist, Verantwortung übernimmt[128] sowie gerne und auch selbstständig arbeitet, weshalb die Kontrollen und die Lenkung seitens der Vorgesetzten unangebracht sind.[129] Die Theorie Y geht davon aus, dass die Unternehmens- und Individualziele miteinander verschmelzen.[130] Als möglicher Führungsstil kristallisiert sich die Führung durch Motivation heraus. McGregor selbst präferierte die Theorie Y, welche normative Züge trägt.[131] Nach McGregor führt die Unterstellung unterschiedlicher Menschenbilder seitens der Führungskräfte zum entsprechenden Verhalten bei den Mitarbeitern,[132] somit avancieren die angenommenen Menschenbilder zu einer Self-Fulfilling-Prophecy.[133]
Die wichtigsten Annahmen der Theorien sind in Tabelle XXX dargestellt:

Tabelle 10: Annahmen der Menschenbild Theorie X und Theorie Y nach McGregor[134]

Theorie X	Theorie Y
• Der Durchschnittsmensch hat eine angeborene Abneigung gegen Arbeit und versucht, ihr aus dem Weg zu gehen, wo er nur kann. • Weil der Mensch durch Arbeitsunlust gekennzeichnet ist, muss er zumeist gezwungen, gelenkt, geführt und mit Strafe bedroht werden, um ihn mit Nachdruck dazu zu bewegen, das vom Unternehmen gesetzte Soll zu erreichen. • Der Durchschnittsmensch zieht es vor, an die Hand genommen zu werden, möchte sich vor der Verantwortung drücken, besitzt verhältnismäßig wenig Ehrgeiz und ist vor allem auf Sicherheit aus.	• Die Verausgabung durch körperliche und geistige Anstrengungen beim Arbeiten kann als ebenso natürlich gelten, wie Spiel oder Ruhe • Von anderen überwacht und mit Strafe bedroht werden ist nicht das einzige Mittel, jemanden zu bewegen, sich für die Ziele des Unternehmens einzusetzen; ein verpflichtendes Ziel führt zu Selbstdisziplin und Selbstkontrolle • Wie sehr er sich Zielen verpflichtet fühlt, ist eine Funktion der Belohnung, die mit ihrem Erreichen verbunden ist • Der Durchschnittsmensch lernt unter geeigneten Bedingungen, Verantwortung nicht nur zu übernehmen sondern sogar zu suchen • Die Anlage zu einem hohen Grad von Vorstellungskraft, Urteilsvermögen und Erfindungsgabe ist in der Bevölkerung weit verbreitet • Unter den Bedingungen der industriellen Arbeitswelt wird das Potential an Verstandeskräften, über das der Durchschnittsmensch verfügt, nur zum Teil genutzt.

Menschenbildtypologie nach Edgar E. Schein

Edgar E. Schein[135] „ordnete […] seine vier Typen in der Reihenfolge ihres Auftretens in der Literatur“[136] und nimmt ebenso wie McGregor an, dass Manager explizite oder implizite An-

[125] Auf Maslows Bedürfnispyramide wird bei Hesch (1997), S. 90ff., Engelkamp/Sell (2005), S. 12f. und Hungenberg/Wulf (2007), S.269ff. näher eingegangen.
[126] Vgl. Hesch (1997), S. 93.
[127] Vgl. Weinert (1995), Sp. 1500.
[128] Vgl. Blickle (2004), Sp. 837.
[129] Vgl. Neuberger (2006), S. 346.
[130] Vgl. Steinle (1978), S. 191.
[131] Vgl. Steinle/Ahlers (2004), Sp. 1145.
[132] Vgl. Hesch (1997), S. 95.
[133] Vgl. Scholz (2000), S. 119, Hesch (1997), S. 95 sowie Spector (1996), S. 361.
[134] Eigene Darstellung in Anlehnung an McGregor (1970), S. 47f. und S. 61f.
[135] Edgar E. Schein ist emeritierter Professor für Organisationspsychologie und Management am MIT.
[136] Matthiesen (1995), S. 77.

nahmen über ihre Angestellten treffen; daher beeinflussen die unterschiedlichen Menschenbilder das Führungsverhalten der Vorgesetzten. [137]

Die Annahmen des *„rational-economic man"* folgen aus denen des homo oeconomicus.[138] Die Handlungsmaxime dieses Menschenbildes lautet: „der Mensch analysiert seine Handlungsmöglichkeiten, wählt diejenige Alternative aus, die seinen Zielen am besten entspricht und handelt dementsprechend."[139] Der rational-economic man stimmt im Wesentlichen mit McGregors Theorie X überein und kann nur durch monetäre Anreize motiviert werden.[140] Die Handlungen der Mitarbeiter müssen durch das Management gleichermaßen geplant, organisiert und kontrolliert werden, da diese selbst passiv sind.[141]

Der *„social man"* wird durch dominierende, soziale Motive, einer Sinnerfüllung der Arbeit nur über soziale Kontakte und einer Abhängigkeit von Gruppennormen bei der Leistungserstellung geprägt.[142] Eine positive Einstellung des Mitarbeiters kann nur erwartet werden, wenn die Führungskräfte seinem Verlangen nach sozialen Bedürfnissen und Akzeptanz entgegen kommt.[143] Mittels Gruppenanreizsystemen lässt sich der social man motivieren. Der Vorgesetzte muss fähig sein, die Bedürfnisse nach sozialer Anerkennung, Zugehörigkeit und Identität zu befriedigen, um die Akzeptanz der Unternehmensziele zu gewährleisten.[144]

Das Menschenbild des *„self-actualizing man"* stimmt mit den Annahmen von McGregors Theorie Y überein.[145] Der self-actualizing man strebt nach Selbstverwirklichung. Er trachtet danach, seine Aufgaben stets zu erledigen, und versucht, seine Fähigkeiten durch neue sowie umfangreichere Aufgaben zu erweitern.[146] Autonomie ist sein Ziel, welches durch Selbstkontrolle und Selbstmotivation erreicht werden kann, ohne einen Konflikt zwischen Unternehmenszielen und Zielen des self-actualizing man hervorzurufen.[147] Aufgabe der Führungskraft ist es, einen Sinn in den Aufgaben zu vermitteln, der den einzelnen mit Stolz und Selbstachtung erfüllt. Der Manager übernimmt die Aufgabe eines Katalysators und Förderers und nicht mehr die des Motivators und Kontrolleurs.[148]

Das Konstrukt des *„complex man"* wurde von Schein selbst entwickelt und sollte alle vorherigen Konstrukte in sich integrieren.[149] Es „geht von einem *situativen Ansatz* aus, bei dem in Abhängigkeit von den persönlichen Merkmalen des Mitarbeiters (Eigenschaftsansatz) und in Abhängigkeit von der Führungssituation (Situationsansatz) eine individuelle und zeitpunktbezogene Form der Führung gewählt werden muss."[150] Denn der Mitarbeiter ist an sich ein komplexes, vielschichtiges und wandlungsfähiges[151] Wesen, dessen Motivstrukturen situativen wie auch zeitlichen Änderungen und Anpassungen unterliegen.[152]

---

[137] Vgl. Scholz (2000), S. 120.
[138] Vgl. Scholz (2000), S. 121.
[139] Steinle (1978), S. 193.
[140] Vgl. Steinle (1978), S. 193.
[141] Vgl. ebenda, S. 78.
[142] Vgl. Steinle (1978), S. 193.
[143] Vgl. ebenda, S. 193.
[144] Vgl. Matthiesen (1995), S. 78 und Staehle (1999), S. 194.
[145] Vgl. Staehle (1999), S. 195.
[146] Vgl. Steinle (1978), S. 193.
[147] Vgl. Stahle (1999), S. 195.
[148] Vgl. Schein (1980), S. 69.
[149] Vgl. Matthiesen (1995), S. 77.
[150] Scholz (2000), S. 122, (Hervorhebung im Original).
[151] Vgl. Scholz (1994), S. 407.
[152] Vgl. Steinle (1978), S. 194.

Unterschiedliche Motive führen zu differenzierten und uneinheitlichen Führungsstilen, die je nach Individuum und Situation angepasst werden müssen. Es lässt sich somit kein eindeutiges Führungsverhalten identifizieren. Es obliegt den Führungskräften, den entsprechenden Führungsstil zur Motivation und Führung der Mitarbeiter zu finden.[153]

Das Menschenbild des complex man belegt „die Hypothese, dass Menschenbilder in der BWL dem Menschen nicht gerecht werden."[154] Denn Menschenbilder sind Verallgemeinerungen und eine Reinform nur eines Menschenbildes bei den Mitarbeitern zu identifizieren, dürfte fast unmöglich sein, jedoch ist die Auseinandersetzung mit ihnen wichtig, um die Mitarbeitermotivation und deren Anreize zu erkunden.[155]

Tabelle 11: Menschenbilder und deren unterschiedliche organisatorische Konsequenzen nach Schein[156]

Menschenbild	Organisatorische Konsequenzen
1. rational-economic man Ist in erster Linie durch monetäre Anreize motiviert, ist passiv und wird von der Organisation manipuliert, motiviert und kontrolliert; sein Handeln ist rational; Annahmen der Theorie X.	Klassische Management-Funktionen: Planen, Organisieren, Motivieren, Kontrollieren; Organisation und deren Effizienz stehen im Mittelpunkt, Organisation hat die Aufgabe, irrationales Verhalten zu neutralisieren und zu kontrollieren.
2. social man In erster Linie durch soziale Bedürfnisse motiviert; als Folge der Sinnentleerung der Arbeit wird in sozialen Beziehungen am Arbeitsplatz Ersatzbefriedigung gesucht; wird stärker durch soziale Normen seiner Arbeitsgruppe als durch Anreize und Kontrollen des Vorgesetzten gelenkt; Annahmen der Human-Relations-Bewegung.	Aufbau und Förderung von Gruppen; soziale Anerkennung der Mitarbeiter durch Manager und Gruppe; die Bedürfnisse nach Anerkennung, Zugehörigkeitsgefühl und Identität müssen befriedigt werden; Gruppenanreizsysteme treten an die Stelle von individuellen
3. self-actualizing man Menschliche Bedürfnisse lassen sich in einer Hierarchie anordnen, der Mensch strebt nach Autonomie und bevorzugt Selbst-Motivation und Selbst-Kontrolle; es gibt keinen zwangsläufigen Konflikt zwischen Selbstverwirklichung und organisatorischer Zielerreichung; Annahmen der Theorie Y.	Manager sind Unterstützer und Förderer (nicht Motivierer und Kontrolleure); Delegation von Entscheidungen; Übertragung von Amts-Autorität zu Fach-Autorität, Übergang extrinsischer Motivation zu intrinsischer Motivation; Mitbestimmung am Arbeitsplatz.
4. complex man Ist äußerst wandlungsfähig, die Dringlichkeit der Bedürfnisse unterliegt Wandel, der Mensch ist lernfähig, erwirbt neue Motive; in unterschiedlichen Systemen werden unterschiedliche Motive bedeutsam; Annahmen der Situationstheorie.	Manager sind Diagnostiker von Situationen; sie müssen Unterschiede erkennen können und Verhalten situationsgemäß variieren können; es gibt keine generell richtige Organisation.

Menschen müssen motiviert und kontrolliert werden, um ihre Arbeit schnell, zuverlässig und pflichtbewusst zu erledigen. Nur dann steuern sie ihren Beitrag zur Erreichung der Unternehmensziele bei. Der Faktor Mensch gehört daher in einem ganzheitlichen Sicherheitskonzept berücksichtigt, welches im Folgenden entwickelt wird.

[153] Vgl. Kirchler et al. (2004), S. 120.
[154] Matthiesen (1995), S. 103.
[155] Vgl. Suter (1999), S. 138.
[156] Eigene Darstellung in Anlehnung an Staehle (1999), S. 195f. nach Schein (1980), p. 52-72 und p. 93-101.

5 Informationssicherheit in ITIL V3

5.1 Sicherheitspolitik, Sicherheitskonzept und Sicherheitskultur

Ein wichtiger Bestandteil einer Unternehmung zur Selbstdefinition und zur Beschreibung der eigenen langfristigen Zielsetzung ist die Unternehmenspolitik. Es ist „die Gesamtheit der grundlegenden Entscheide, welche das Unternehmensgeschehen in die Zukunft hinein auf längere Frist in den wesentlichen Grundlinien bestimmen sollen."[157]
Einen Teilbereich der Unternehmenspolitik stellt die Sicherheitspolitik dar. Sie bildet die Grundlage für jene Aktivitäten in einer Unternehmung, die dafür Sorge tragen, dass ein reibungsloser IT-Betrieb gewährleitstet werden kann, indem Risiken für die Informationssicherheit minimiert sowie die Verarbeitung und Speicherung von Daten garantiert werden.[158] In der Sicherheitspolitik werden „die durch die Unternehmensleitung definierten strategischen Ziele, Grundsätze und Richtlinien des Sicherheitsmanagement verankert."[159] Die Sicherheitspolitik muss in Einstimmung mit der Unternehmenspolitik erarbeitet und schriftlich fixiert werden, wobei hier ein Sicherheitsniveau spezifiziert werden sollte, welches von der Organisation und den Mitarbeitern auch erreicht werden kann.[160]
Für die Umsetzung der strategischen Ziele der Sicherheitspolitik auf der operativen Ebene bedarf es eines Sicherheitskonzeptes. Dieses „konkretisiert die Sicherheitspolitik einer Unternehmung und dient der Übersetzung der auf strategischer Ebene festgesetzten Sicherheitsziele, -grundsätze und -richtlinien in Maßnahmen, die sich auf konkrete Gefährdungsebenen und Sicherheitsaspekte beziehen."[161] Das Sicherheitskonzept stellt einen ganzheitlichen Rahmen für ein unternehmensspezifisches Sicherheitsmanagement dar.[162]
Ganzheitlich bedeutet, bei einem Sicherheitskonzept nicht nur in technische Maßnahmen (wie Hard- und Software) zu investieren[163] sondern auch gleichermaßen in die Mitarbeiter. Eine Investition in die Hard- und/oder Software kann enorm viel Sicherheit bieten, jedoch kann das beste Sicherheitssystem seine Aufgaben nicht wahrnehmen, wenn es durch die Belegschaft auf Grund von Fahrlässigkeit oder Irrtum unterwandert und somit außer Kraft gesetzt wird. Der Mensch bietet die Grundlage für eine ganzheitliche Problemlösungsmethodik, da er sich vielfältigen Problemsituationen gegenüber gestellt sieht.[164] Eine deutliche Steigerung des Sicherheitsniveaus kann realisiert werden, indem den Menschen bzw. Mitarbeitern die notwendigen Informationen gegeben und entsprechende Handlungsweisen vermittelt, vorgelebt und diese trainiert werden.

Um eine Sicherheitskultur in einer Unternehmung zu implementieren, muss diese aus der jeweiligen Unternehmenskultur abgeleitet werden.[165] Die Unternehmenskultur ist „die **Gesamtheit von Grundannahmen, Werten und Normen**, die in einer Unternehmung gemeinsam akzeptiert und gelebt werden. Kultur resultiert einerseits aus dem Handeln der Unterneh-

[157] Ulrich (1990), S. 11.
[158] Vgl. Hoppe/Prieß (2003), S. 280.
[159] Hoppe/Prieß (2003), S. 281.
[160] Vgl. ebenda, S. 281.
[161] Ebenda, S. 282.
[162] Vgl. ebenda, S. 282. Weiterhin
[163] Vgl. Sitzberger/Nowey (2006), S. 1f.
[164] Vgl. Steinle (2005), S. 45.
[165] Vgl. Schlienger (2003), S. 35.

mungsmitglieder und steuert umgekehrt ihr Verhalten. Sie konkretisiert sich in **Symbolen** als sichtbare Ausdrucksformen."[166]
Im Kern einer jeden Unternehmenskultur stehen die grundlegenden Annahmen über die Natur der Menschen, deren Verhalten sowie deren Beziehung. Diese Annahmen manifestieren sich in den Werten, Normen und Wissensbeständen von Unternehmen und kommen durch Artefakte und Kreationen wie Handbücher, Rituale oder Anekdoten zum Ausdruck. Eine Subkultur der Unternehmenskultur ist die Sicherheitskultur. Diese unterstützt, dass die Informationssicherheit ein natürlicher Aspekt der täglichen Arbeit jedes Mitarbeiters wird und hilft dabei, das nötige Vertrauen zwischen den diversen Partnern einer Unternehmung aufzubauen.[167]
Nach Hoppe und Prieß stellt die Sicherheitskultur „die Gesamtheit der in einer Unternehmung vorherrschenden kollektiven Werte, Normen, Traditionen, Überlieferungen und Denkhaltungen dar, die sämtlichen Mitgliedern einer Unternehmung Sinn und Richtlinien für ihr Verhalten im Zusammenhang mit der Sicherheit der in der Unternehmung existierenden IS vermittelt."[168] Sie bedarf einer vielfältigen Kommunikation bezüglich der sicherheitsrelevanten Fragen und es werden in Unternehmungen viele Diskurse benötigt, damit sich gemeinsame Werte und Normen entfalten, wobei jeder Mitarbeiter seinen Teil zur Kultur beiträgt.[169]

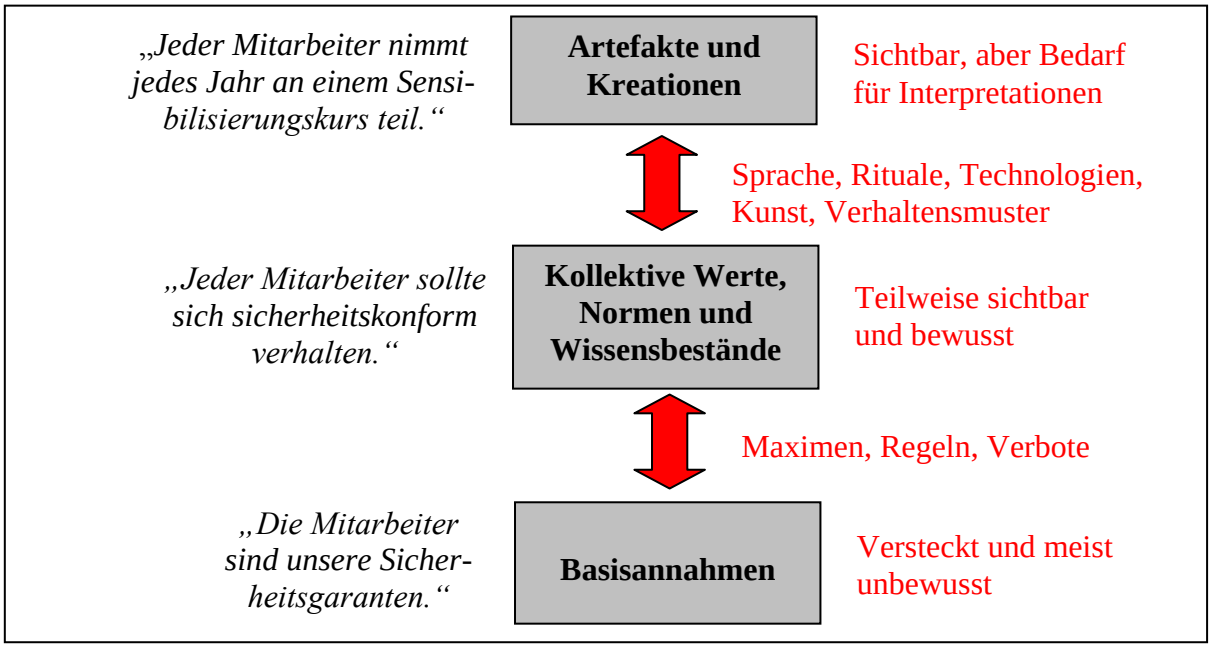


Abbildung 6: Ebenen der Sicherheitskultur mit Beispielen[170]

Abbildung 6 wurde in Anlehnung an Edgar E. Schein mit Beispielen für die Informationssicherheit versehen. Schein unterscheidet drei Ebenen der Kultur, die sich auf den Grad der Sichtbarkeit von kulturellen Phänomenen beziehen, wobei die einzelnen Ebenen in einer Wechselwirkung zueinander stehen. Die Artefakt-Ebene zeigt die sichtbaren, spürbaren und offenkundigen Erscheinungsformen einer Gruppe (Kleidung, Rituale und Sprechweisen). Diese Ebene wird durch zwei immaterielle Ebenen komplettiert. Zum einen durch die Ebene der

[166] Steinle (2005), S. 99 (Hervorhebungen im Original).
[167] Vgl. Schlienger (2003), S. 35.
[168] Hoppe/Prieß (2003), S. 289.
[169] Vgl. Buerschaper (2008), S. 165.
[170] Eigene Darstellung in Anlehnung an Schlienger (2003), S. 35 nach Schein (1995), S. 30.

Normen, Werte und Wissensbestände und zum anderen durch die der Basisannahmen, die die Kulturessenz darstellen. Letztere Ebene ist essentiell, da sie innerhalb der Unternehmung tief fixiert und unbewusst ist und daher als ungeschriebenes Gesetz gilt.[171]

Durch die Implementierung einer Sicherheitskultur[172] kann die Sensibilität der Mitarbeiter für Risiken gesteigert werden. Sie ist maßgebend für die Art und Weise der Kommunikation von Chancen und Risiken innerhalb einer Unternehmung. Die Sicherheitskultur ist zu einem Sammelbegriff für ein pro-aktives und ganzheitliches Handeln avanciert, welches dazu dient, den Sicherheitsgedanken und das Sicherheitsverständnis in einer Unternehmung zu erweitern. Ziel der Sicherheitskultur ist es, eine Koordinationsfunktion sowie eine Integrationsfunktion zu ermöglichen. Die Koordinationsfunktion sorgt für eine Zeit- und Reaktionsersparnis sowie für eine Vergrößerung der Widerstandsfähigkeit, indem auf einheitliche kulturelle Werte innerhalb der Unternehmung, unabhängig von unvorhersehbaren Situationen und Entscheidungen, zurückgegriffen werden kann. Weiterhin werden formale Regelungen und administrative Anweisungen minimiert. Eine Sicherheitskultur muss in einer Unternehmung von allen Mitarbeitern gelebt werden, sie muss einheitlich sein und darf nicht durch andere Subkulturen unterwandert werden. Die Integration der Sicherheitskultur bildet ein übergeordnetes Element, welches es ermöglicht, dass (pro-)aktiv gehandelt und der Sicherheitsgedanke in einer Unternehmung aktiv weiter entwickelt wird. Laut Studien sind ca. 80 bis 90% aller Fehler in IT-Systemen menschbedingt, d. h. dass der Mensch Hauptverursacher von Verletzungen der Informationssicherheit ist. Um erfolgreich Fehler beseitigen zu können, muss der Mensch aus seinen Fehlern lernen.[173]
Die Unternehmenskultur vermittelt den Sinn der Arbeit und steigert somit die Leistungsfähigkeit und -bereitschaft der Mitarbeiter (Motivationsfunktion). Eine ähnliche motivierende Funktion leistet auch die Sicherheitskultur, denn sie vermittelt den Sinn der Sicherheit.[174]
Dieser Sinn spiegelt sich in Verhaltensregeln der Mitarbeiter wieder, die einen Teil der Sicherheitskultur darstellen. Die Mitarbeiter müssen die Wichtigkeit von Verhaltensregeln, wie die Prüfung von Datenträgern auf Viren, die Verschlüsselung von E-Mails und der Anhängen, keine Notierung der Passwörter und die Auswahl geeigneter Passwörter mit kryptischen Zeichen und Sonderzeichen einsehen und diese leben. Sie dürfen nicht vom Management aufoktroyiert werden, da sie sonst ihre Wirkung nicht entfalten können.[175]

5.2 ITIL V3

Die IT Infratructure Library (ITIL) „ist ein Referenzmodell für das Management von (internen) IT-Dienstleistungen im Unternehmen.“[176] Aufgabe von ITIL ist die Definition und Beschreibung von good practices für die zentralen Prozesse der Bereitstellung von IT-Services, wie das Problem-, Change-, Konfigurations-[177] und das Sicherheitsmanagement.

[171] Vgl. Schlienger et al. (2004), S. 9f.
[172] Zur Implementierung einer Sicherheitskultur und deren einzelne Schritte und Maßnahmen sowie zur Kontrolle der Sicherheitskultur siehe Schlienger et al. (2004).
[173] Vgl. hierzu Schlienger et al. (2004), S. 11-19.
[174] Vgl. Scholz (2000), S. 782.
[175] Vgl. Rautenstrauch/Schulze (2003), S. 206.
[176] Krcmar (2005), S. 39.
[177] Vgl. Krcmar (2005), S. 39.

ITIL ist in mehrere Module bzw. Disziplinen zu einem Regelwerk zusammengefasst, welches bei stetiger Umsetzung die Leistungsfähigkeit der Unternehmens-IT erhöht und folglich die Nutzung der IT-Ressourcen und die Qualität der IT-Services steigert. Ein wichtiges Element ist der Bezug auf die jeweiligen Geschäftsprozesse der Unternehmung sowie die Konzentration auf die IT-Services, die die Geschäftsprozesse effektiv bzw. bestmöglich unterstützen.[178]
Wesentliche Ziele von ITIL sind

- *die Erhöhung der Qualität,*
- *die Verstärkung der Standardisierung,*
- *die Kostensenkung und*
- *die Messbarkeit von Leistung.*[179]

ITIL V3 beschreibt das „WAS" (Prozesse, Rollen, Aufgaben und Abhängigkeiten) jedoch nicht das „WIE" (Implementierungsvorschriften oder Tools) des Servicemanagement.[180] Letzteres ist auf die jeweilige Unternehmung, deren Größe, Unternehmenskultur und Anforderungen abzustimmen und entsprechend umzusetzen.[181]
ITIL V3 ist in fünf Kernbereiche unterteilt (vgl. Abb. 7): Service Strategies, Service Design, Service Transition, Service Operation und Continual Service Improvement, die jeweils ein Kerngebiet abdecken und einen Servicelebenszyklus darstellen.
„Service Strategy ist die Achse des Servicelebenszyklus […], welche alle anderen Phasen antreibt; es ist die Phase, die Richtlinien und Ziele setzt. Die Phasen Service Design, Service Transition und Service Operation werden von dieser Strategie geführt. Ihr fortwährendes Motiv ist Anpassung und Veränderung. Die Phase Continual Service Improvement steht für Lernen und Verbesserung und umschließt alle anderen Lebenszyklus-Phasen."[182]

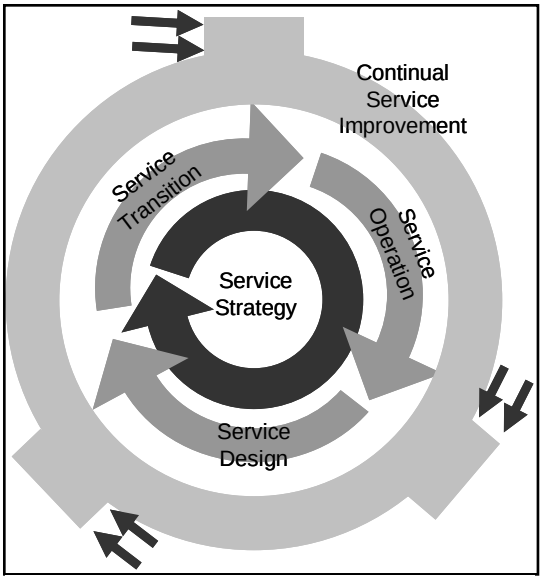


Abbildung 7: ITIL Servicelebenszyklus
Quelle: eigene Darstellung in Anlehnung an OGC (2007a), S. 8

5.3 Information Security Management in ITIL V3

Das Information Security Management (ISM) beschreibt im De-facto-Standard ITIL die elementaren prozessualen Anforderungen.[183] Durch das Management muss dabei eine strategische Ausrichtung der Sicherheitsaktivitäten erfolgen, um die Sicherheitsziele zu erreichen. Weiterhin gilt es, Sicherheitsrisiken effizient zu managen. Ziel des ISM ist, alle Aspekte der IT-Sicherheit bereitzustellen und die Schutzmaßnahmen zu koordinieren. Zur Gewährleistung der Sicherheitseffektivität gilt es, eine end-to-end Betrachtung der Geschäftsprozesse vorzu-

[178] Vgl. Kopperger et al. (2007), S. 138.
[179] Kopperger et al. (2007), S. 139 (Hervorhebung im Original).
[180] Vgl. Olbrich (2008), S. 1.
[181] Vgl. Kopperger et al. (2007), S. 140.
[182] Bon, von (2008), S. 22.
[183] Vgl. Böttcher (2008), S. 69.

nehmen.[184] Die IT-Sicherheitsanforderungen leitet das ISM aus den Compliance Anforderungen, den gesetzlichen Vorschriften sowie den Sicherheitsrichtlinien der Unternehmung ab, woraufhin notwendige Schutzmaßnahmen entwickelt werden. Das ISM beschränkt sich auf die Gewährleistung der Vertraulichkeit, der Verbindlichkeit sowie der Integrität von Informationen und legt zusammen mit den Verantwortlichen und Auftraggebern die zu schützenden Informationen fest.[185] Vier Schutzmaßnahmenkategorien werden unterschieden:[186]

- *personelle* Schutzmaßnahmen (z. B. Verfahrensanweisungen, Schulungen der Mitarbeiter sowie Awareness Kampagnen)
- *technische* Schutzmaßnahmen (z. B. Virenschutz und Firewalls)
- *prozessuale* Schutzmaßnahmen (z. B. Sperrung eines Zuganges nach wiederholter Falscheingabe des Passwortes
- *physikalische* Schutzmaßnahmen (z. B. Zutritts- und Zugriffskontrollen)

ITIL V3 stellt sich als ganzheitliches Sicherheitskonzept dar, weil es sich nicht mit isolierten Maßnahmen, die in den seltensten Fällen effektiv sind,[187] begnügt, sondern Wert auf ein ausgewogenes Konzept, bestehend aus prozessualen, physikalischen, technischen und personellen Schutzmaßnahmen, gelegt wird.

Information Security Management System

„Das Information Security Management System (ISMS) ist jener Teil des übergreifenden Managementsystems, der die Organisationsstruktur, Regelungen, Abläufe sowie Ressourcen zur Entwicklung, Umsetzung, Bewertung und Aufrechterhaltung der Information Security Policy beinhaltet und dokumentiert. Zielsetzung des Einsatzes eines Information Security Management System ist es, innerhalb eines gegebenen Organisationsbereichs eine angemessene Informationssicherheit zu schaffen und aufrechtzuerhalten.“[188]

Das ISMS beinhaltet den Informationssicherheitsprozess, der aus den Teilprozessen Planung, Implementierung, Bewertung und Wartung bzw. Gewährleistung der Informationssicherheit besteht. Abbildung 8 verdeutlicht diesen Prozess.[189]

Die Phase *Steuerung* dient der Erstellung eines Management Frameworks, das die Informationssicherheit initiiert und steuert. Es dient weiterhin der Errichtung einer Organisationsstruktur, die die Informationssicherheitspolitik vorbereitet, anerkennt und implementiert und der Zuweisung von Verantwortung an die Mitarbeiter.

In der Phase *Planung* werden geeignete Maßnahmen zur Gefahrenabwehr erarbeitet. Die Anforderungen werden aus Geschäfts- und Servicerisiken, Plänen und Strategien, SLAs und der legalen, moralischen und ethischen Verantwortung für die Informationssicherheit abgeleitet.

Die Phase *Implementierung* zielt darauf ab, sicherzustellen, dass geeignete Verfahren, Werkzeuge und Kontrollen vorhanden sind, die die Informationssicherheitspolitik unterstützen.

---

[184] Vgl OGC (2007b), S. 141.
[185] Vgl. Böttcher (2008), S. 70.
[186] Vgl. hierzu und im Folgenden Böttcher (2008), S. 71.
[187] Vgl Böttcher (2008), S. 71.
[188] Ebel (2008), S. 295.
[189] Der Prozess leitet sich von Demings Qualitätszyklus ab, der für eine kontinuierliche Verbesserung der Prozesse sorgt. Für vertiefende Informationen vgl. Ebel (2008), S. 296-300 und BSI (2008), S. 14-16. Vgl. im Folgenden OGC (2007b), S. 143-144.

Die Phase *Bewertung* dient der Überwachung und Kontrolle der Einhaltung der Sicherheitsanforderungen in den SLAs, sowie der Überprüfung der technischen Sicherheit der IT-Systeme. Die Phase *Wartung* zielt auf das Lernen aus Fehlern ab, um eine Verbesserung der Sicherheit zu erlangen.

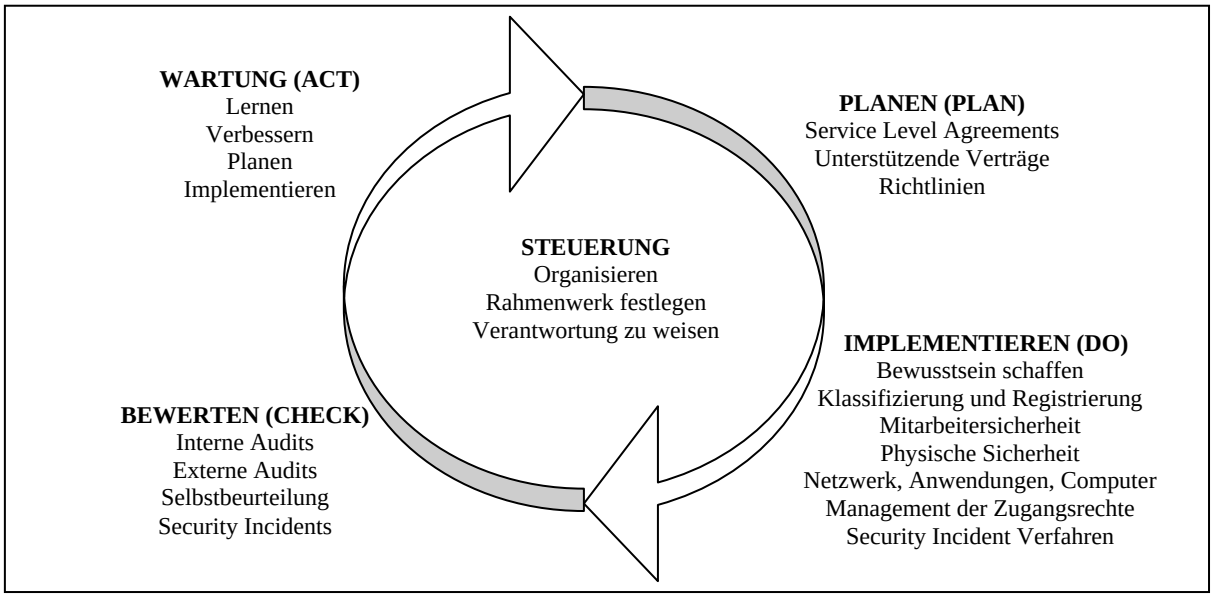


Abbildung 8: Framework zur Steuerung der IT-Sicherheit in ITIL V3[190]

Hauptbestandteil des vorgestellten Frameworks ist die Ermittlung, Implementierung und Verbesserung der Informationssicherheitspolitik.

Informationssicherheitspolitik

Die Aktivitäten des ISM sollten mittels einer unternehmensweiten Informationssicherheitspolitik (ITP) sowie unterstützender spezifischer Sicherheitsrichtlinien gebündelt und ausgeführt werden. Die ITP unterstützt dabei die allgemeine Unternehmenssicherheitspolitik sowie die Anforderungen der Unternehmensführung. Die ITP und die ergänzenden Richtlinien müssen innerhalb der Unternehmung einen weiten Mitarbeiterkreis ansprechen und ihnen zur Verfügung gestellt werden. Ebenso müssen sie innerhalb der SLA‘s umgesetzt werden. Die Sicherheitspolitik ist eine Managementaufgabe, sie muss daher vom Management autorisiert und vorangetrieben werden. Für die Einhaltung der Sicherheitspolitik bedarf es einer regelmäßigen Kontrolle, um eventuelle Abweichungen feststellen und neue Aspekte aufnehmen zu können.[191]

Prozessaktivitäten, Methoden und Techniken

Das ISM hat das vorrangige Ziel, die Sicherheitsaspekte unter Berücksichtigung der IT-Services zu gewährleisten und alle Aktivitäten dementsprechend zu steuern und zu kontrollieren. Schlüsselaktivitäten sind:[192]

[190] Eigene Darstellung in Anlehnung an OGC (2007b), p. 143 sowie Bon, von (2008), S. 105.
[191] Vgl. OGC (2007b), S. 142.
[192] Vgl. hierzu und im Folgenden OGC (2007b), S. 144.

- Erarbeitung, Überprüfung und Revision einer umfassenden ITP und unterstützender spezifischen Richtlinien sowie die Kommunikation, Implementierung und Durchsetzung der ITP.
- Bewertung und Klassifizierung der Informationen.
- Umsetzung, Überprüfung, Überarbeitung und Verbesserung der Sicherheitskontrollen sowie der Risikobewertung und der Reaktion auf Bedrohungen.
- Überwachung und Management aller Sicherheitsverletzungen und wichtiger sicherheitsrelevante Ereignisse
- Analysen, Berichterstattung und Reduzierung der Sicherheitsverletzungen und deren Folgen.

Die Informationssicherheit ist ein sich ständig ändernder Prozess, da stets neue Bedrohungen auftreten können, die bis dato noch nicht bekannt gewesen sind.[193]

Sicherheitskontrollen in ITIL V3

Die Sicherheitskontrollen unter ITIL sind derart zu gestalten, dass sie die ITP unterstützen. Die in Abbildung 9 veranschaulichten Sicherheitsvorfälle (Incidents) werden primär durch menschliche Fehler und nicht durch technische Gefahren verursacht. Zu Beginn dieses Prozesses steht ein Risiko, welches eine Gefahr oder Bedrohung darstellt, also einen negativen Einfluss ausüben könnte. Realisiert sich diese Bedrohung, spricht man von einem Sicherheitsvorfall. Dieser Vorfall widerum kann einen Schaden hervorrufen, welcher behoben werden muss. Je nach Wichtigkeit lassen sich unterschiedliche Maßnahmen ergreifen:[194]

- *Vorbeugende Maßnahmen* versuchen den Eintritt zu verhindern.
- *Reduzierende Maßnahmen* dienen dazu, das Ausmaß eines Schadens zu begrenzen.
- *Detektivische Maßnahmen* spüren Sicherheitsvorfälle auf.
- *Repressive Maßnahmen* stellen die Auswirkungen ab.
- *Korrigierende Maßnahmen* stellen den ursprünglichen Zustand wieder her.

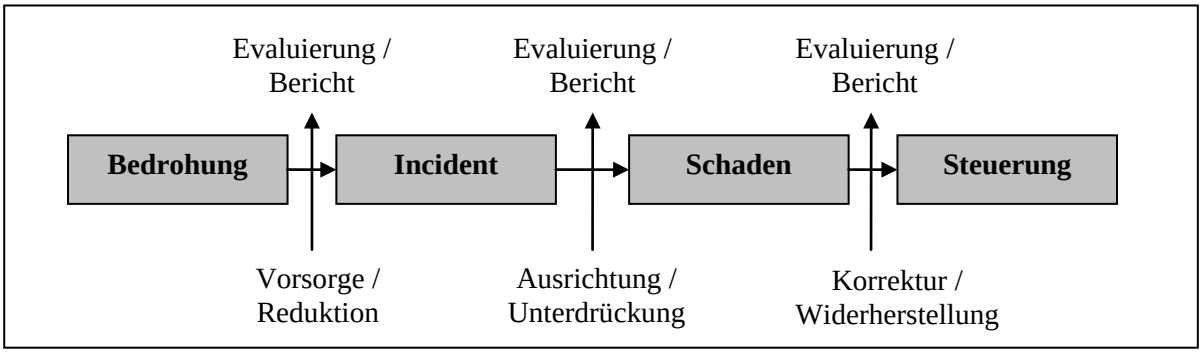


Abbildung 9: Kontrolle von Bedrohung und Incident[195]

Fehlende Aspekte der Sicherheit in ITIL V3

Im Rahmen des ISM werden die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit angesprochen, die die Informationssicherheit der Assets, Informationen, Daten und IT-

[193] Vgl. Bon, van (2008), S. 105.
[194] Vgl, hierzu und im Folgenden OGC (2007b), S. 145f. und Bon, van (2008), S. 106.
[195] Eigene Darstellung in Anlehnung an OGC (2007b), S. 145.

Services garantieren,[196] jedoch nicht die Authentizität oder die Verbindlichkeit. Die Sicherheitsziele einer Organisation umfassen häufig alle fünf Sicherheitszielen und nicht nur aus den in ITIL V3 genannten.
Ein vollendendes Sicherheitskonzept ist in ITIL V3 nicht vorhanden. Das Framework zur Steuerung der IT-Sicherheit bietet erste Ansätze. Es wird in der Phase Implementierung von Awareness Konzepten gesprochen.[197] In den Verantwortungsbereich des Sicherheitsmanagers fällt es, eine Informationssicherheitspolitik zu entwickeln und zu veröffentlichen, [198] jedoch reicht eine ITP alleine nicht aus, um das Thema Sicherheit fest in den Köpfen der Mitarbeiter zu verankern.
Auf Grund der dargestellten Mängel wird im Folgenden ein Konzept erstellt, welches den Mitarbeiter als zentralen Punkt sieht, um die Informationssicherheit zu gewährleisten. Neben den personellen sind ebenso technische, prozessuale und physikalische Maßnahmen von Bedeutung. Es gilt hierbei, das schwächste Glied (die Mitarbeiter) zu stärken, indem deren Sicherheitsbewusstsein gekräftigt[199] sowie deren Motivation im Umgang mit dem Thema Sicherheit erhöht wird. Neben diesen Maßnahmen kann die Informationssicherheit durch andere flankierende Maßnahmen zu akzeptablen Kosten auf das angestrebte Sicherheitsniveau angehoben werden.

6 Erstellung eines ganzheitlichen Sicherheitskonzeptes

6.1 Auswahl geeigneter Schutzmaßnahmen

Zum Schutz der Informationen und IT-Systeme ist ein ganzheitliches Konzept erforderlich, welches über die Anschaffung von Firewalls, Anti-Virenprogrammen und Backupsystemen hinausgeht und weitere Aspekte (vor allem das Personal) einbezieht. Nur auf diese Weise kann der jeweilige Schutzbedarf eines Unternehmens festgestellt werden.[200]

Das ganzheitliche Sicherheitskonzept (vgl. Abb. 10) basiert auf der *Unternehmenskultur*, welche die *Unternehmenspolitik* und -*strategie* umgibt. Aus der *Unternehmenskultur* bildet sich die *Sicherheitskultur*. Aus der *Unternehmenspolitik* wird die langfristige *Unternehmensstrategie* abgeleitet;[201] aus dieser lässt sich die *Sicherheitsstrategie* entwickeln.[202] Eine Dreiecksverbindung aus *Unternehmenspolitik, Unternehmenskultur* und *Sicherheitskultur* bildet das Gerüst für die Schaffung der *Sicherheitspolitik*. Aus der *Sicherheitspolitik* und den *Sicherheitsrichtlinien* kann die *Sicherheitsstrategie* unter Einbezug der *Unternehmensstrategie* entwickelt werden. Das *Sicherheitsmanagement* (ISM) bricht die *Sicherheitspolitik* in operative Maßnahmen herunter, welche wiederum geplant, umgesetzt und kontrolliert werden müssen. Im Folgenden werden einzelne Aspekte des Konzepts skizziert:

[196] Vgl. Buchsein et al. (2008), S. 69 sowie Böttcher (2008), S. 70.
[197] Vgl. OGC (2007b), S. 143 und Abb. 4.26.
[198] Vgl. OGC (2007b), S. 144.
[199] Vgl. Lardschneider (2008), S. 575 und Hoppe/Prieß (2003), S. 199.
[200] Vgl. Münch (2007), S. 289.
[201] Vgl. Steinle (2005), S. 302.
[202] Vgl. Bock et al. (2008), S.135.

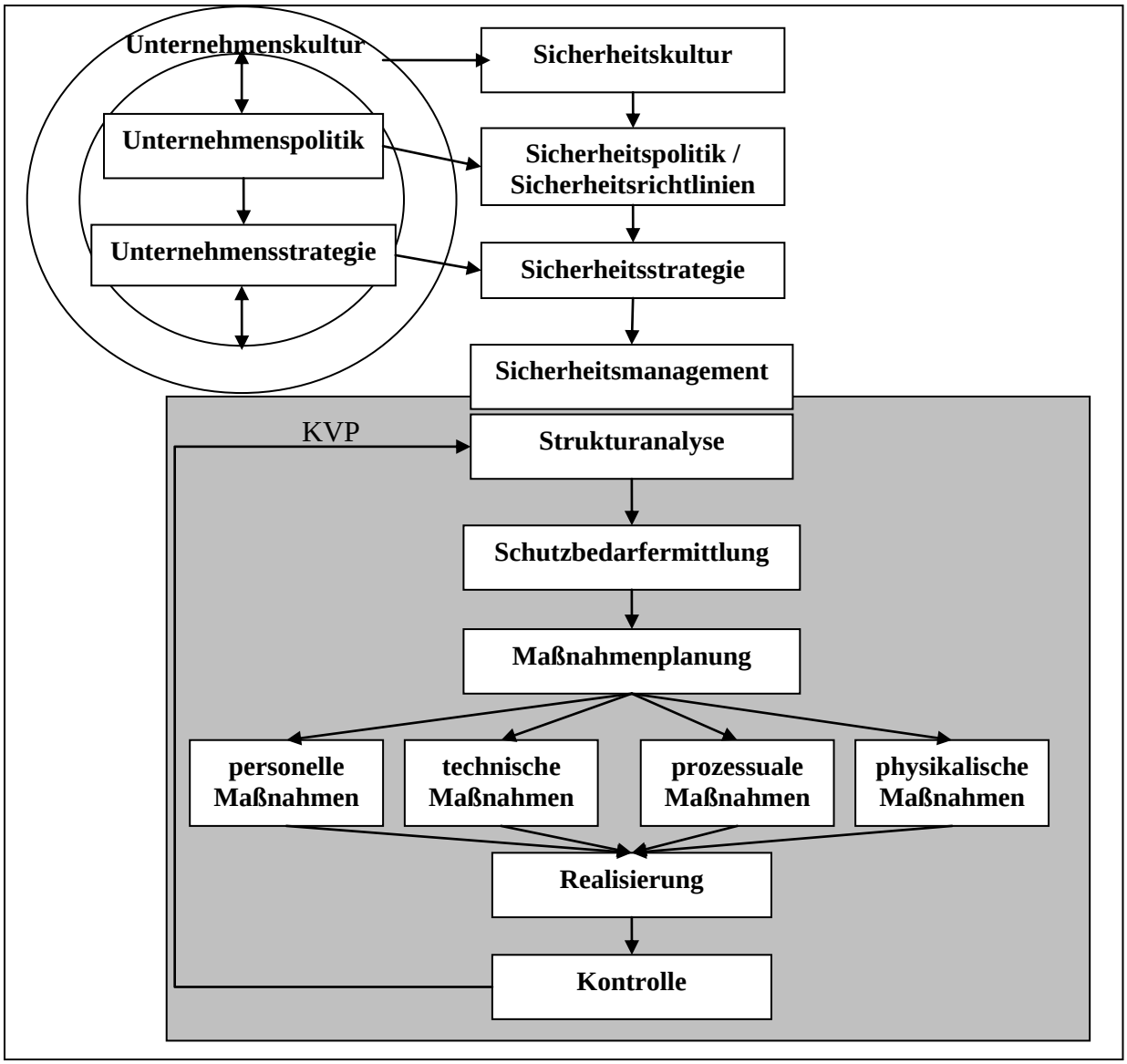


Abbildung 10: Ein ganzheitliches Sicherheitskonzept[203]

Mittels der **Strukturanalyse** werden essentielle Informationen für das weitere Vorgehen im Rahmen des Sicherheitskonzeptes gesammelt. Ziel ist es, alle Bestandteile zu erfassen, die für die Ausführung geschäftskritischer Geschäftsprozesse oder Fachaufgaben notwendig sind. [204] Um eine Komplexitätsreduktion zu erreichen, sollten ähnliche Objekte in Gruppen zusammen gefasst werden. Stichprobenartig ist es nun möglich, den Sicherheitszustand einer Gruppe zu identifizieren, da die Gruppen die gleichen Eigenschaften besitzen.[205] Aus einem Soll-Ist-Vergleich von empfohlenen Schutzmaßnahmen und den in dem Unternehmen bereits implementierten lässt sich ein Plan für fehlende und/oder mangelhafte Schutzmaßnahmen ableiten.[206]

[203] Eigene erweiterte Darstellung in Anlehnung an BSI (2008a) S. 36 und Steinle (2007), S. 146.
[204] Dieses sind z. B. wichtige Informationen, Anwendungen, IT-Systeme, Rollen, Kommunikationsnetze, die Räumlichkeiten ebenso wie die Infrastruktur des Unternehmens, die eingesetzte Hard- und Software, Anwendungsdaten, Prozesse und Personen. Vgl. BSI (2008a) S. 39; Bitkom (o. J.), S. 16
[205] Vgl. ebenda, S. 40.
[206] Vgl. Rauschen/Dister (2004), S. 27.

In das Sicherheitskonzept sollten auch die in der Planung befindlichen IT-Systeme, Anwendungen und Räume ebenso wie das Personal mit einbezogen werden.[207] „Ziel ist die Schaffung einer soliden Grundlage, in der alle sicherheitsrelevanten Parameter beschrieben sind“[208] sowie die Nutzung dieser Daten für den Gewährleistung und die kontinuierliche Verbesserung der Informationssicherheit.

Bei der **Schutzbedarfsermittlung** werden die in der Strukturanalyse ermittelten Schwachstellen im Hinblick auf deren Vertraulichkeit, Integrität und Verfügbarkeit überprüft und in die Schadenskategorien *normal*, *hoch* und *sehr hoch* eingestuft.[209]
Neben den technischen Aspekten, wie den Anwendungen, deren räumliche Verteilung und Vernetzung, ist auch der Schutzbedarf in Bezug auf das jeweilige Personal zu ermitteln.
Bei einem *normalen bis mittleren* Schutzbedarf, reicht häufig eine Mitarbeiterschulung bezüglich der Aufgaben, Informationen und Anwendungen, um diese ohne Fehler bedienen und verarbeiten zu können. Eine Schulung und Sensibilisierung des gesamten Personals in Bezug auf die Informationssicherheit[210] und deren weit reichende Konsequenzen bei Nichteinhaltung von gewissen Sicherheitsvorkehrungen ist ebenso anzuraten wie eine wiederkehrende Verinnerlichung durch Programme und Plakate. Weiterhin ist eine formelle und rechtliche Bindung der Mitarbeiter im Umgang mit Daten, Vorschriften und Regelungen, sowie die PC-Nutzung, Regelungen für die Internet-Nutzung[211] und die private E-Mail-Nutzung zu schaffen.
Wird der Schutzbedarf als *hoch* eingestuft, sollten vertiefende Schulungen erfolgen, um den Mitarbeitern die möglichen Folgen von Fehlverhalten und Irrtümern zu veranschaulichen. Dabei ist es essentiell, den Organisationsmitgliedern zu verdeutlichen, dass Sie eine sehr wichtige Position innehaben, die mit großer Verantwortung Ihren Kunden und der gesamten Organisation gegenüber verbunden ist.
Für Schutzbedarfe, die als *sehr hoch* und damit als besonders kritisch eingestuft werden, reichen oben genannte Maßnahmen der geringeren Schutzbedarfe nicht mehr aus. Das Personal ist nicht nur zu schulen und zu sensibilisieren, es sind darüber hinaus intrinsisch motivierte, loyale und zuverlässige Mitarbeiter auszuwählen. Um Irrtümer und Fehler auszuschließen, wäre eine Überprüfung der Arbeiten durch einen gleichgestellten, qualifizierten und motivierten Kollegen sinnvoll.

Die **Maßnahmenplanung** folgt der Erfassung der bereits implementierten Schutzmaßnahmen erfasst. Ziel ist eine weitere Steigerung der Sicherheit. Die in ITIL V3 angesprochenen Schutzmaßnahmen lassen sich in personelle, technische, physikalische und prozessuale Maßnahmen gliedern. Die personellen Maßnahmen werden in ITIL V3 vernachlässigt und werden im Rahmen dieses Konzeptes verstärkt herausgestellt. Jedoch dürfen diese nicht losgelöst von den technischen, physikalischen und prozessualen Maßnahmen implementiert werden, so dass auf diese ergänzend eingegangen werden soll.

[207] Vgl. Münch (2007), S. 290f.
[208] Münch (2007), S. 291.
[209] Vgl. Hofmann (2007a), S. 255.
[210] Vgl. Pohlmann/Blumberg (2006), S. 414.
[211] Vgl. Pohlmann/Blumberg (2006), S. 415.

Personelle Maßnahmen sind alle Schutzmaßnahmen, „die *an* Personen ausgeführt werden, um sie für die Bedeutung der IS-Sicherheit zu sensibilisieren, zur Gewährleistung von IS-Sicherheit zu qualifizieren sowie zu motivieren bzw. zu verpflichten.“[212] Dies schließt den Umgang mit Daten, Informationen, Anwendungen aber auch die Handhabung von E-Mail-Programmen, die Internetnutzung sowie den Schutz vor Angriffen mit ein. Die Art und die Anwendung der personellen Maßnahmen sind an die jeweiligen Bedürfnisse der unterschiedlichen Menschenbilder der Mitarbeiter anzupassen. Nicht jede Maßnahme ist geeignet, um die spezifischen Belange der unterschiedlichen Charaktere der Mitarbeiter im geforderten Sinne zu beeinflussen. So muss zwischen den Anreizen, der Motivation und dem Führungsstil der unterschiedlichen Menschenbilder differenziert werden. Des Weiteren kann bereits bei der Mitarbeiterauswahl je nach Menschenbild entschieden werden, ob diese Person den Anforderungen, die an die Informationssicherheit gestellt werden, genügt.
Bei den Mitarbeitern muss zwischen dem Wollen und dem Können, wie Abbildung 11 zeigt, unterschieden werden. Unter *Können* werden die Fähigkeiten eins Mitarbeiters zusammengefasst, die für eine adäquate Bewältigung der Arbeit und der Einhaltung der Sicherheit verantwortlich sind.[213] Als Maßnahmen zur Steigerung des Könnens kristallisieren sich die Qualifikation durch Schulungsmaßnahmen, Awareness Kampagnen, die Unterstützung durch das Management sowie die Auswahl geeigneter Mitarbeiter heraus.

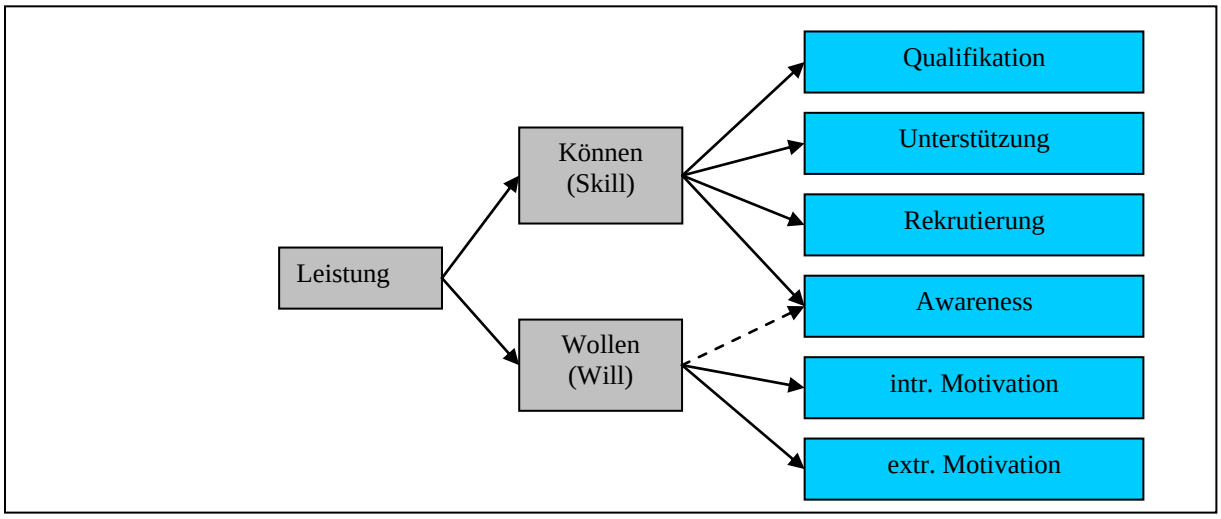


Abbildung 11: Maßnahmen zur Steigerung des Könnens und des Wollens von Mitarbeitern[214]

Neben der Fähigkeit eines Mitarbeiters, die ihm übertragenen Aufgaben zu erfüllen, stellt sich die Frage des *Wollens*, also ob ein Mitarbeiter die Aufgaben im Sinne des Unternehmens bewältigen will. Meist stellt ein Mitarbeiter nicht sein volles Leistungspotential für die Aufgabenbewältigung bereit, jedoch ist es möglich, durch extrinsische und intrinsische Motivation und deren Anreize das Leistungspotential zu steigern.[215]
So sind je nach Wissenstand unterschiedliche Maßnahmen zu ergreifen, um bei allen Mitarbeitern das gleiche Sicherheitsbewusstsein und -verhalten zu erreichen.

[212] Hoppe/Prieß (2003), S. 199 (Hervorhebung im Original).
[213] Vgl. Ridder (2007), S. 288.
[214] Eigene Darstellung.
[215] Vgl. Ridder (2007), S. 288.

Es ist empfehlenswert, seine Mitarbeiter zu motivieren, denn motivierte Mitarbeiter kümmern sich um die Belange des Unternehmens, zu denen sowohl die Aufgabenbewältigung als auch eine gewissenhafte und sicherheitskonforme Bewältigung der Aufgaben zählt.
Motivation[216] ist ein „Zustand des inneren »Angetriebenseins« einer Person. Dies kann auch über externe Anreize beeinflusst werden. Die aktuellen Motivationsinhalte basieren auf individuellen Lebens-, Arbeits-, und Berufswerten sowie der grundsätzlichen Orientierung an Aufgaben, Personen und Institutionen.“[217]
Motivation wird in der Fachliteratur in intrinsisch und extrinsisch unterteilt. Unter *intrinsischer Motivation* werden „interessensbezogene Handlungen verstanden, die keiner externen Anstöße bedürfen. Sie werden um ihrer selbst willen unternommen. Intrinsische Motivation beinhaltet Neugier, Exploration, Spontanität und Interesse an der unmittelbaren Umwelt und stellt den Inbegriff des selbstbestimmten Verhaltens dar. Das Individuum fühlt sich frei in der Auswahl und Durchführung seiner Handlungen. Das Handeln stimmt mit dem eigenen Willen überein.“[218] *Extrinsische Motivation* dagegen wird als „Handeln verstanden, das mit instrumenteller Absicht durchgeführt wird, um andere Ziele zu erreichen. Es erfolgt selten spontan und wird meist durch Aufforderung in Gang gesetzt, die eine Bekräftigung (z. B. Belohnung) darstellen.“[219]

Tabelle 12: Motivationsmöglichkeiten der Menschenbilder[220]

Menschenbild	Motivation	Anreize
rational-economic man / Theorie X	extrinsisch	finanzielle Anreize (Entlohnung, Gratifikationen), Kontrolle, Druck
social man	intrinsisch	Gruppenbildung, Wir-Gefühl, Zufriedenheit, soziale Anerkennung
self-actualizing man / Theorie Y	intrinsisch	Selbstmotivation, Selbstkontrolle durch Delegation, Autonomie, Mitbestimmung am Arbeitsplatz
complex man	intrinsisch	vielfältige Arten der Motivation

Die Motivation erfolgt mittels Anreizen. Die Anreize lassen sich grob in materielle und immaterielle unterteilen,[221] wobei bei den immateriellen zwischen sozialen Anreizen, Anreizen aus der Arbeit selbst und Anreizen des organisatorischen Umfeldes unterschieden wird.[222]
Anreize haben eine dreifache Funktion. Sie besitzen eine Aktivierungsfunktion von Motiven der Mitarbeiter, eine Zufriedenheitsfunktion durch Erfüllung der Motive und eine Leistungsfunktion durch Erzeugung von Ergebnissen, die die wirtschaftliche Leistung der Unternehmen steigern.[223]

[216] In der Literatur werden unterschiedliche Motivationstheorien angesprochen. Zum einen die Inhaltstheorien, wie die Bedürfnistheorie nach Maslow und die Zwei-Faktoren Theorie nach Herzberg. Diese versuchen zu erklären, welche Faktoren beim Menschen ein bestimmtes Verhalten auslösen. Zum anderen die Prozesstheorien (wie z. B. die VIE-Theorie von Vroom), die Aussagen darüber treffen, wie die Motivation initiiert, erhalten und bewertet wird. Vgl. Staehle (1999), S. 221ff., Drumm (2008), S. 391ff. und Oechsler (2005), S. 340ff.
[217] Wunderer (2007), S. 104.
[218] Ridder (2007), S. 299.
[219] Ridder (2007), S. 299.
[220] Eigene Darstellung in Anlehnung an Scholz (2004), S. 407.
[221] Vgl. Drumm (2008), S. 458.
[222] Vgl. v. Rosenstiel (1975), S. 231.
[223] Vgl. Steinle (1978), S. 62.

Bezogen auf die oben genannten Menschenbilder kann demzufolge der *rational-economic man*, bzw. das Menschenbild, nach der Theorie X extrinsisch durch finanzielle bzw. monetäre Anreize wie Belohnung aber auch durch Druck und Kontrolle zur Arbeit bzw. dazu, sich sicherheitskonform zu verhalten, motiviert werden.
Das Menschenbild des *social man* vermag motiviert werden, indem Gruppen gebildet werden, in denen ein Wir-Gefühl geschaffen wird. Das um den Mitarbeiter herum aufgebaute soziale System ist in der Lage, die Bedürfnisse des social man nach sozialer Nähe und Kooperation mit anderen zu befriedigen. Diese Anreize helfen dem social man, die ihm übertragenen Arbeiten, schnell und zügig zu erledigen sowie die Sicherheitsvorschriften zu beachten.
Durch intrinsische Anreize wie die Aufgabenvielfalt und die Tätigkeit an sich kann der *self-actualizing man* sowie das Menschenbild der Theorie Y motiviert werden. Die Mitarbeiter nach diesem Typus sind in der Lage, sich durch die Tätigkeit selbst zu motivieren und sich auch selbst zu kontrollieren. Die ihnen übertragenen ganzheitlichen Aufgaben werden durch die Führungskräfte an sie delegiert. Die Delegation[224] spielt bei der Motivation des self-actualizing man eine bedeutende Rolle, so bedarf es also keiner Motivation durch extrinsische Anreize wie beispielsweise Geld. Wird die intrinsische Motivation durch eine extrinsische Belohnung ersetzt, so würde erstere untergraben werden.[225]
Der *complex man* sieht sich einer Vielzahl von Motiven gegenüber, die sich je nach System und Situation ändern, daher ist es kompliziert für diesen Typus die geeigneten Anreize zu identifizieren und anzuwenden. Die Führungskraft, ist in Bezug auf diesen Typus Mensch, Diagnostiker der Situationen. Sie muss in der Lage sein, Unterschiede zu erkennen und ihr Verhalten situationsgemäß anzupassen, da der complex man besonders wandlungsfähig ist. Für dieses Menschenbild existiert kein einheitlicher Führungsstil.[226]

Weiterhin ist es möglich, durch die Etablierung einer Sicherheitskultur die Mitarbeiter bezüglich der Informationssicherheit zu motivieren. Besonders bereits in dem Unternehmen tätige Mitarbeiter gilt es in Bezug auf die Informationssicherheit zu motivieren. Bei neu einzustellenden Mitarbeitern ist es empfehlenswert, Können und Wollen in Bezug auf die Sicherheit zu überprüfen. Es ist denkbar, dass unmotivierte und Personen mit unzureichender Einstellung gar nicht erst in ein Arbeitsverhältnis kommen, welches ihren Vorstellungen von Sicherheit widerspricht.[227]
Abbildung 12 zeigt, dass Menschenbilder vom Typus X/rational-economic man eher nicht eingestellt werden, da sie unmotiviert und böswillig sind und sich zudem sicherheitswidrig verhalten. Dagegen sollten Mitarbeiter des Typus Y eingestellt und motiviert werden, da sie gutwillig und von vornherein motiviert sind sowie sich sicherheitskonform verhalten. Den indifferenten Mitarbeiter wie den social man gilt es einzustellen und durch oben genannte Anreize zu motivieren.

[224] Delegation lässt sich „als eine auf Dauer angelegte Übertragung von Aufgaben, Kompetenzen und Verantwortung begreifen, die sich im Verhältnis zwischen Delegierendem und Delegationsempfänger realisiert und auf das Schaffen zurechenbarer Handlungsspielräume gerichtet ist.“ Bruch (1996), S. 15.
[225] Vgl. Nerdinger (2004), S. 93 sowie Deci/Ryan (1993), S. 226.
[226] Vgl. Staehle (1999), S. 195.
[227] Vgl. Schlienger (2003), S. 34.

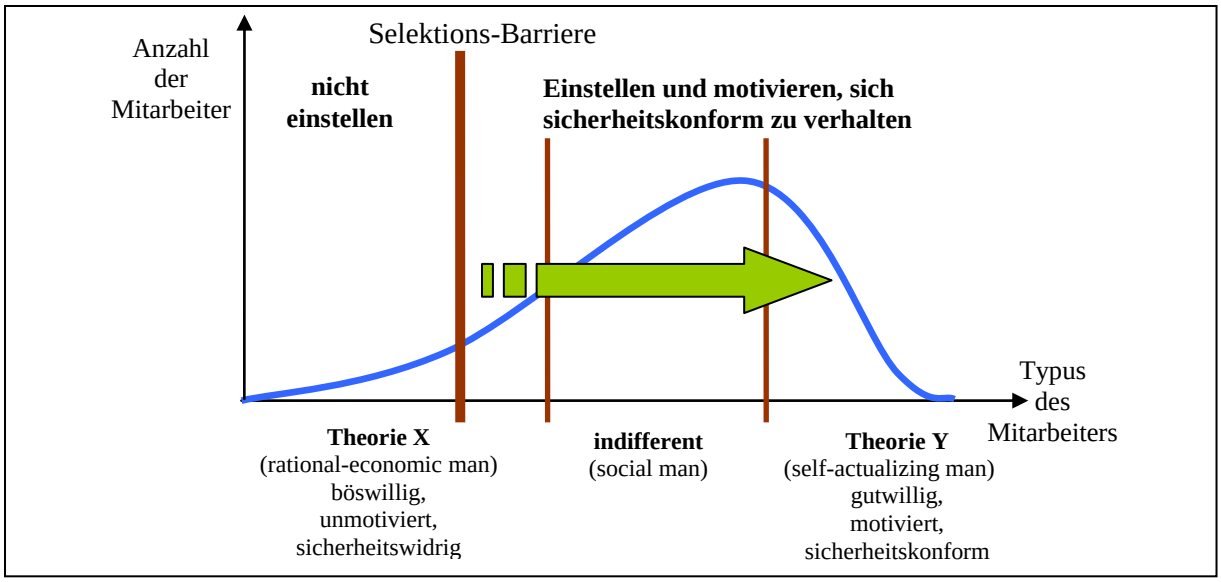


Abbildung 12: Selektion und Motivation von Mitarbeitern[228]

Die Motivation und die Fähigkeiten eines Mitarbeiters werden durch den Führungsstil mit geprägt und beeinflusst. Ein einheitlicher Führungsstil kann nicht angewendet werden, da die Mitarbeiter eines Unternehmens unterschiedliche Motivationen und Fähigkeiten aufweisen. Ein situatives Modell der Führung ist das Reifegradmodell von Hersey und Blanchard. Bei diesem Modell existiert eine prägende Komponente, der aufgabenrelevante Reifegrad der Mitarbeiter.[229] Der Reifegrad lässt sich zum einen in die psychologische Reife (der Wille bzw. die Motivation zu handeln) und zum anderen in die psychologische Reife (die Professionalität, die Kompetenz und das Commitment[230]) unterteilen.[231]

Die Reifegradtheorie beschreibt vier unterschiedliche Führungsstile (FS), von denen je nach Reifegrad des Mitarbeiters einer von der Führungskraft gewählt wird (vgl. Abb. 13).

Beim *autoritären Führungsstil* („telling“) gibt die Führungskraft die Tätigkeiten und den Zeitpunkt der Fertigstellung für Mitarbeiter mit einem geringen Reifegrand wie dem rational-economic-man vor. Bei reiferen Mitarbeitern wie dem social man wird der *integrierende Führungsstil* („selling“) angewendet, der den Versuch unternimmt, die Meinungen der Mitarbeiter zu berücksichtigen, jedoch trifft letztlich die Führungskraft die Entscheidung. Beim *partizipativen Führungsstil* („participating“) spielt der Mitarbeiter mit zunehmender Reife bei der Entscheidungsfindung sowie bei der Durchführung eine tragende Rolle. Der Führungsstil berücksichtigt bei der Entscheidungsfindung sowohl die Meinungen der Mitarbeiter als auch die der Führungskraft. Der *delegierende Führungsstil* („delegating“) wird bei extrem reifen Mitarbeitern (self-actualizing man) angewendet, die über eine hohes Maß an Motivation und Qualifikation verfügen.[232]

Ziel der Führungskraft ist es, ihre Mitarbeiter so zu motivieren und zu fördern, dass sie diese nur noch nach dem delegierenden Führungsstil führt.[233]

---

[228] Eigne Darstellung in Anlehnung Schlienger (2003), S. 35.
[229] Vgl. Scholz (2000), S. 943.
[230] Commitment ist die Selbstverpflichtung auf die Ziele des Unternehmens. Vgl. Steinle et al. (1999), S. 225.
[231] Vgl. Hinterhuber (2004), S. 163.
[232] Vgl. Scholz (2005), S. 944 und Oechsler (2005), S. 370.
[233] Vgl. Oechsler (2005), S. 370.

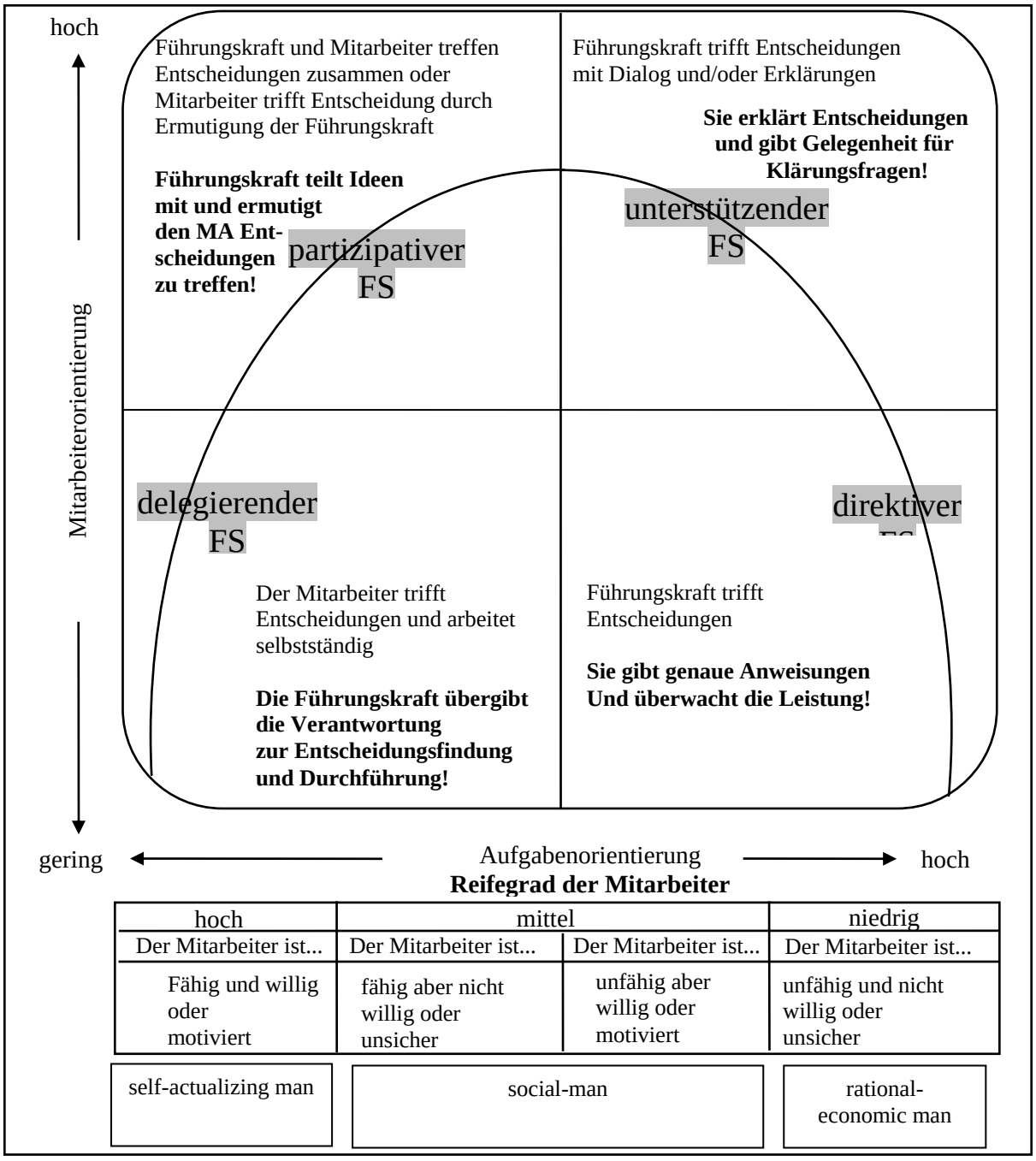


Abbildung 13: Reifegradtheorie nach Hersey und Blanchard[234]

Die Reifegradtheorie stellt weitreichende Anforderungen an die Führungskräfte.[235] Sie ermöglicht es den Führungskräften, die Mitarbeiter individuell, entsprechend ihrer Bedürfnisse, nach Führung und Motivation anzuleiten und vor allem auch, durch stufenweise Delegation von Aufgaben und Verantwortlichkeiten den Reifegrad sukzessive zu steigern.

Bereits durch die Auswahl eines geeigneten Führungsstils für den einzelnen Mitarbeiter zeigt sich die Unterstützung des Managements. Diese Maßnahme alleine ist noch nicht zielführend, denn es bedarf nicht nur einer Führung und Motivation der Mitarbeiter, sondern eines Vorle-

[234] Eigene Darstellung in Anlehnung an Hentze et al. (2005), S. 295f. und Scholz (2000), S. 943 nach Hersey/Blanchard (1982), S. 248/S. 299.
[235] Vgl. Scholz (2000), S. 944.

bens der Informationssicherheit durch die Vorgesetzten, die den Mitarbeiter den Sinn und die Auswirkungen im Schadensfall der Informationssicherheit vermitteln. Die Sinnvermittlung wird bereits durch die Sicherheitskultur unterstützt, die Regeln im Umgang mit der IT, den Daten und Informationen werden im Rahmen der Informationssicherheitspolitik und den jeweiligen Sicherheitsrichtlinien näher spezifiziert.
Die Aufgaben des Managements umfassen die Umsetzung der Informationssicherheitspolitik, die Erarbeitung und Kontrolle von geeigneten Maßnahmen sowie die Qualifikation der Mitarbeiter. Vorgesetzte können ein sicherheitskonformes Verhalten belohnen und Sicherheitsübertretungen sanktionieren. Fehler machen und diese einzugestehen ist ein positives Verhalten, das belohnt werden sollte. Wenn Absicht oder Böswilligkeit den Mitarbeitern unterstellt werden kann, sind Sanktionsmaßnahmen anzuraten.[236]
Nimmt das Management an Schulungen teil, ist es den Mitarbeitern eine Vorbildfunktion; zudem kann sich das Management mit dem Thema auseinandersetzen und die eigene Motivation stärken. Aufgabe des Managements ist es, vor Eintritt eines schädigenden Ereignisses Vertretungsregelungen zu erstellen, um den Betrieb der IT und der Informationssicherheit bei Personalausfall zu gewährleisten.[237]

Die Kompetenzen der Mitarbeiter können durch Schulungs- und Trainingsmaßnahmen gesteigert werden. Das Können bzw. die Fähigkeiten der Mitarbeiter im Zusammenhang mit der Informationssicherheit können durch Mitarbeiterschulungen verbessert werden. Die Qualifikation „von Mitarbeitern umfasst Maßnahmen zum Aufbau, Erhalt und Ausbau von Fähigkeiten und Fertigkeiten, die zur Bewältigung von tätigkeitsspezifischen Anforderungen notwendig sind.“[238] Eine einführende Schulung für neue Mitarbeiter in die grundlegenden und insbesondere sicherheitsrelevanten Arbeitsabläufe ihres neuen Arbeitsplatzes ist anzuraten. Prinzipiell sollten Systemnutzer, Entwickler, Anwender und das Management regelmäßig in Bezug auf ihr Aufgabengebiet geschult werden. [239] Eine Gewährleistung der Informationssicherheit ist nur gegeben, wenn jeder beteiligte und involvierte Mitarbeiter einen angemessenen Wissensstand über Informationssicherheit hat; dieser Wissenstand sollte allgemeine und explizite Gefahren und Bedrohungen im eigenen Verantwortungsbereich der Mitarbeiter abdecken.[240]
In einer Schulung sind den Mitarbeitern die mitarbeiterbezogenen Schutzmaßnahmen näher zu bringen, denn eine effektive Umsetzung der mitarbeiterbezogenen Maßnahmen kann meist erst nach einer Schulung und Motivation erfolgen. Neben den mitarbeiterbezogenen Maßnahmen sollten auch produktbezogene Maßnahmen vermittelt werden. Der Umgang mit diesen Schutzmaßnahmen muss den Mitarbeitern gezielt beigebracht werden. Ferner sind ihnen der korrekte Einsatz und die adäquate Nutzung von Zugangscodes und Zugangskontrollmedien zu vermitteln. Die Wichtigkeit der regelmäßigen Durchführung von Datenbackups, der Verschlüsselung von zu übertragenden Daten sowie die Handhabung von personenbezogenen Daten ist den Mitarbeitern näher zu bringen, ebenso wie das Vorgehen bei Notfällen bzw. Incidents. Aufgabe der Schulung ist die Inhaltsvermittlung der Sicherheitspolitik sowie der weiteren Sicherheitsrichtlinien, die einem sicheren Umgang mit dem Internet sowie der siche-

[236] Vgl. Schlienger (2003), S. 34f.
[237] Vgl. Pohlmann (2006), S. 416f.
[238] Hoppe/Prieß (2003), S. 200.
[239] Vgl. Hoppe/Prieß (2003), S. 200f.
[240] Vgl. Pohlmann (2006), S. 418.

ren Nutzung der E-Mail-Konten dienen. Ferner sind alltägliche Richtlinien, die Bestandteil des Arbeitsvertrages sein sollten, wie die Sperrung des PCs beim Verlassen des Büros, das Verschließen von Schubläden und Schränken, das unter Verschlusshalten von vertraulichen Daten bei Abwesenheit sowie der Umgang mit Passwörtern nochmals anzusprechen.[241]
Ergänzende Schulungen sind für Administratoren und eventuelles Wartungspersonal durchzuführen.[242]

Zur Unterstützung der Schulungen bieten sich Sensibilisierungsmaßnahmen wie Awareness bildende Kampagnen an. Sensibilisierungsmaßnahmen der Mitarbeiter sind notwendig, um Fehlerquellen zu bekämpfen.[243] Für ein Sicherheitskonzept spielt die Förderung des Sicherheitsbewusstseins eine große Rolle.[244] Die Awareness Kampagne kann als Schlüsselelement der Informationssicherheit angesehen werden.[245] Sicherheitsbewusstsein kann definiert werden als „die gedankliche Auseinandersetzung eines Mitarbeiters mit den Risiken, die sich aus unvorhergesehenen externen Ereignissen („höhere“ Gewalt), kriminellen Energien anderer Menschen oder aus seinem eigenen (Fehl-)Verhalten im Umgang mit Arbeitsergebnissen, eingesetzten Arbeitsmitteln und Technologien für seinen Arbeitgeber hinsichtlich der angestrebten Unternehmensziele ergeben können.“[246] Security Awareness Kampagnen sind im Rahmen eines Sicherheitsmanagements unabdingbar[247] und sollten folglich in ein Sicherheitskonzept mit aufgenommen werden.
Vielen Managern ist bewusst, dass durch die Erhöhung des Sicherheitsbewusstseins der Mitarbeiter das gesamte Sicherheitsniveau erhöht werden kann, da viele Sicherheitsmaßnahmen einer aktiven und positiven Unterstützung der Mitarbeiter bedürfen. Ziel einer solchen Kampagne ist es, eine langfristige Verhaltensänderung der Mitarbeiter zu initiieren. Der Inhalt der Kampagne ergibt sich aus der Informationssicherheitspolitik eines Unternehmens, die Dauer beträgt mehrere Jahre. Die Kampagne durchläuft während dieser Zeit vier Phasen (vgl. Abb. 14).[248]
In Phase 1 wird die Aufmerksamkeit der Mitarbeiter geweckt, indem z. B. Plakate aufgehängt werden. Ferner dient sie dem Zweck, dass sich das Management mit der Kampagne identifiziert und den Inhalt der Kampagne den Mitarbeitern per Rundschreiben näher bringt.
In der Phase 2 wird das notwendige Wissen für das Verständnis von Schutzmaßnahmen vermittelt. Dies geschieht im Rahmen von Informationsveranstaltungen, Intranet-Seiten, Videos, Web Based Trainings und einer Evaluation des Sicherheitsbewusstseins. In dieser wichtigsten Phase soll das Verhalten und die Einstellung der Mitarbeiter langfristig verändert werden, was am einfachsten zu realisieren ist, wenn auch private Sicherheitsinteressen behandelt werden.
Die Phase 3 dient der Verstärkung der zu verändernden Einstellung und des zu verändernden Verhaltens des Mitarbeiters. Hier ist eine permanente Auseinandersetzung mit den relevanten Themen zu gewährleisten, damit die Belegschaft ein starkes Sicherheitsbewusstsein ausbilden und sich in kritischen Situationen professionell verhalten kann. Als Maßnahmen kommen hier

[241] Vgl. SAP (2007), S. 48.
[242] Vgl. Pohlmann (2006), S. 422.
[243] Vgl. Falke (2003), S. 185.
[244] Vgl. Lardschneider (2008), S. 575.
[245] Vgl. Abawajy et al. (2008), S. 475.
[246] Zerr (2003), S. 519.
[247] Vgl. Lardschneider (2008), S. 574.
[248] Vgl. hierzu und im Folgenden Fox (2003), S. 676.

Newsletter, Preisausschreiben oder andere Gewinnspiele, Broschüren, Artikel sowie Mitarbeiteranzeigen zum Einsatz.
Die Phase 4 macht Kampagne in der Öffentlichkeit bekannt, um das Vertrauen der Kunden sowie die Reputation des Unternehmens zu steigern. Möglicherweise hat die Veröffentlichung der Kampagne einen positiven Effekt auf andere Unternehmen, die folglich auch eine Sicherheitskampagne starten.

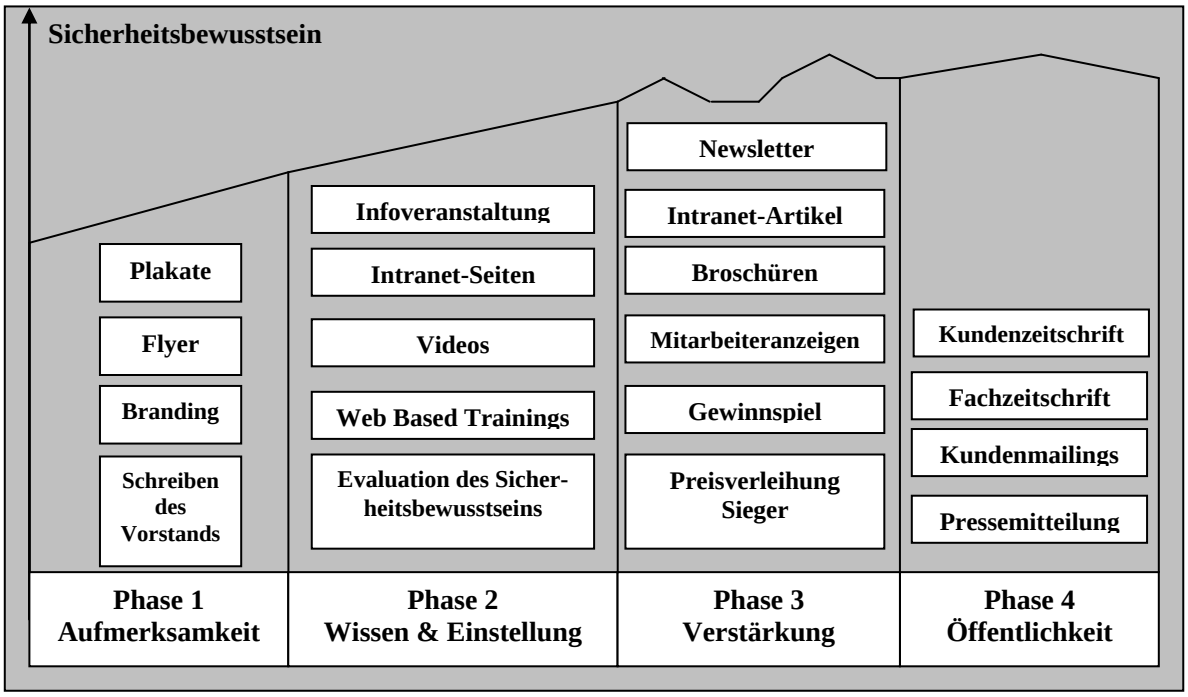


Abbildung 14: Phasen einer Security Awareness Kampagne[249]

Die Verhaltensänderung der Mitarbeiter kann durch Tests und Umfragen, nicht aber mit dem RoSI ermittelt werden. Problematisch ist auch, zu ermitteln, welche Maßnahme der Awareness Kampagne den größten Veränderungseffekt herbeirufen wird.

Neben den personellen Maßnahmen bedarf es weiterer technischer, prozessualer und physikalischer Maßnahmen, die im Folgenden kurz skizziert werden.

Unter **technischen Maßnahmen** werden solche Maßnahmen subsumiert, die die technischen Systeme vor unbefugten Zugriffen durch technische Mittel, wie beispielsweise spezielle Hard- und Software, schützen. Dies umfasst die Sicherung im Rahmen von Angriffen durch Hacker und Cracker sowie Malware aber auch vor Gefahren durch höhere Gewalt. Die Implementierung von technischen Maßnahmen kann einerseits hardwaretechnisch und andererseits softwaretechnisch erfolgen. Die technischen Maßnahmen werden in der folgenden Tabelle überblicksartig dargestellt:

[249] Eigene Darstellung in Anlehnung an Fox (2003), S. 678.

Tabelle 13: Technische Maßnahmen im Rahmen eines ganzheitlichen Sicherheitskonzepts

Antivirensoftware	Malware stellt laut kes Studie 2008 die größte Bedrohung für Unternehmen dar. Um zu verhindern, dass diese Schädlinge in das Unternehmensnetzwerk gelangen, sollten sämtliche Endgeräte mit einem Virenscanner ausgerüstet sein. Eine ständige Aktualisierung der Virendefinition ist unabdingbar.
Firewalls	Die Zugänge zum Internet aber auch zu anderen Firmennetzwerken müssen über Firewalls abgesichert werden, wobei auf ein einheitliches Schutzniveau der Firewalls zu achten ist. Unterschiedliche Firewalls erhöhen das Risiko, dass Angriffe über die schwächste Firewall initiiert werden und somit die qualitativ hochwertigeren Firewalls ausgehebelt werden. Bei der Auswahl des Firewallsystems gilt es zu bedenken, dass ein zentrales Firewallsystem wesentlich effizienter und günstiger ist als eine Firewall, die auf jedem Rechner installiert ist; darüber hinaus lässt sich die Sicherheitspolitik eines Unternehmens durch ein zentrales System auf einfache Weise implementieren. Um ein hohes Sicherheitsniveau zu erreichen, ist es ratsam, neben der zentralen Hardware-Firewall zusätzliche personal Firewalls einzusetzen, die zentral durch einen Administrator verwaltet und konfiguriert werden, wodurch die Sicherheitspolitik schnell, günstig und sicher umgesetzt werden kann.
Intrusion Detection Systeme	Zur Erkennung und zum Entgegenwirken von Angriffe von innen werden Intrusion Detection Systeme (IDS) bzw. Intrusion Prevention Systeme (IPS) verwendet. IDS haben zum Ziel, möglichst früh Angriffe zu identifizieren, um den daraus resultierenden Schaden zu minimieren und den Angreifer zu identifizieren. Des Weiteren erlauben Sie das Aufspüren und die Protokollierung von neuen Angriffsarten, um Präventionsmaßnahmen effektiver gestalten zu können. Bei der Einbruchserkennung wird zwischen der Anomalieerkennungund der Missbrauchserkennung unterschieden. Ein Nachteil von IDS ist, dass sie nur solche Angriffe erkennen und protokollieren, die vorher programmiert werden.
Sicherung von LAN- und WLAN-Verbindungen	Lokale Netzwerke können über Firewalls und Zugriffsbeschränkungen abgesichert werden, gleichermaßen müssen auch die drahtlosen Netzwerke durch sichernde Maßnahmen geschützt werden. Das Medium WLAN nimmt heutzutage einen immer größeren Stellenwert in Unternehmen ein. Die Sicherung der Netzwerkzugänge, sei es über LAN oder WLAN, ist zu gewährleisten, damit keine unbefugten Personen in das Netzwerk eindringen können. Um Angriffe zu verhindern, kann die WLAN-Verbindung mittels Wired-Equivalent-Privacy (WEP), WiFi-Protected-Acces (WPA) oder WPA2 Protokoll verschlüsselt werden. Somit ist es eigentlich nur autorisierten Nutzern möglich, die über das entsprechende Passwort verfügen, sich in das WLAN einzuloggen. Ferner sollten weitere Schutzmaßnahmen wie WLAN-Intrusion Detection und WLAN-Gateways innerhalb eines drahtlosen Unternehmensnetzwerkes zum Einsatz kommen. Weiteren Schutz bietet die Einrichtung eines Virtual Private Networks (VPN): „Ein VPN soll gewährleisten, dass sensible Daten während der Übertragung über Netzwerke (LANs und WANs [und auch WLANs], private und/oder öffentliche Netze) vertrauenswürdig übertragen werden, sodass nur die dazu berechtigten Personen auf die sensiblen Daten zugreifen können.“
Redundanz der Systeme und Daten	Normalerweise sollten Redundanzen von Daten und Systemen vermieden werden. Die Datenredundanz erfordert größere Speicherkapazitäten und weitere Speicherorte. Ähnlich verhält es sich bei der Systemredundanz. Sie verursacht Anschaffungs-, Instandhaltungs- und Wartungskosten. Um jedoch die Verfügbarkeit von Systemen und Daten zu garantieren, die für einen Geschäftsprozess essentiell sind, sollten diejenigen Daten und Systeme redundant vorhanden sein, welche für einen kritischen Geschäftsprozess unabdingbar sind. Bei der redundanten Datenhaltung und bei den redundanten Systemen ist darauf zu achten, dass sowohl die

	Daten als auch die Systeme nicht an dem selben Ort gespeichert und untergebracht sind wie die ursprünglichen Daten und Systeme, damit im Falle einer Katastrophe oder einer Attacke auf die redundanten Daten und Systeme sofort zugegriffen werden kann. Dies ermöglicht einem Unternehmen, seinen Geschäftstätigkeiten auch dann noch nachkommen zu können, wenn ein Zugriff auf ein System und/oder die Daten nicht mehr möglich ist.
Kontinuierliche Datenbackups	Ein weiteres wichtiges Element ist die regelmäßige Sicherung der Daten. Das Backup auf externen Medien dient der Wiederherstellung von Daten, wenn diese durch unbeabsichtigtes Löschen, Manipulation oder durch Zerstörung vernichtet werden. Das Backup zielt auf zwei Schutzziele ab, die Verfügbarkeit von Daten und deren Integrität. Um die Datensicherung vornehmen zu können, müssen entweder die Backups vollkommen automatisiert ablaufen oder aber der Systemadministrator muss eine Zugriffsberechtigung für alle Daten erhalten. Auch die Mitarbeiter, die am Backup beteiligt sind, müssen über eine ausreichende Qualifikation verfügen und die geltenden Sicherheitsvorschriften beachten. Da die zu sichernden Dateien über differenzierte Vertraulichkeitsstufen verfügen, ist es ratsam, die Daten zu verschlüsseln, damit nicht jede Person, die berechtigt ist, auf den Backup Server zuzugreifen, die Daten einsehen und verändern kann.
Erfordernis regelmäßiger Updates und Patches der Software	Zur Systemsicherheit muss auch die Software regelmäßig mit wichtigen Updates und Patches aktualisiert werden. Eine Automatisierung des Updatevorgangs ist riskant, da die Software nicht erkennen kann, ob der Server kompromittiert wurde und manipulierte Updates liefert oder ob sich nicht der Hersteller eine Hintertür (back door) offen hält. Vorteil des Clint Pull-Ansatzes ist dessen Einfachheit, die für Privatanwender ausreicht, allerdings nicht für sichere Systeme in Organisationen. Daher empfiehlt es sich, die Updates durch einen Benutzer oder Administrator zu installieren, der mit der Thematik vertraut ist, nur so können wichtige Updates von unwichtigen unterschieden werden. Eine regelmäßige Suche nach kritischen Updates ist unabdingbar, wobei die Suche mindestens einmal die Woche ausgeführt werden sollte. Kommen extrem kritische Schwachstellen in einer Software zum Vorschein, so werden meist schnell Patches herausgegeben, die diese Schwachstellen beseitigen sollen. Leider geht von diesen Patches eine Fehlerquote von 20% aus, so dass hier weitere Modifikationen erforderlich sind, um diese Fehler zu beheben, die in Form neuer Updates angeboten werden. Bereits bei der Anschaffung von Software ist die Frage zu klären wie lange der Produzent für sein Produkt Support in Form von Updates und Patches leistet.

Im Rahmen der **prozessualen und physikalische Maßnahmen** zählen Rollen und Berechtigungen zu den bedeutsamsten Mitteln. Diese sorgen im Rahmen des gesamten Sicherheitskonzeptes für eine regelkonforme Nutzung der IT-Systeme und deren Daten, wobei sie nicht nur für einzelne Systeme, sondern für das Unternehmen in Gänze vorhanden sein sollten.[250]
In ITIL werden die Aufgaben nicht einzelnen Mitarbeitern sondern Rollen zugeordnet, wobei eine Rolle von einem oder auch von vielen Mitarbeitern wahrgenommen werden kann.[251]

[250] Vgl. Eschweiler/Psille (2006), S. 127.
[251] Vgl. Böttcher (2008), S. 6.

Die Zugriffskontrollen[252] für die Mitarbeiter können in Form von rollenbasierte Zugriffskontrolle (RBAC)[253] oder zentralistisch verpflichtende Zugriffskontrolle (MAC)[254] realisiert werden.[255] Welche Art der Zugriffskontrolle es anzuwenden gilt, ist immer von der jeweiligen Organisation abhängig. Die RBAC sollte in Organisationen eingesetzt werden, in denen die Mitarbeiter häufig in Projekten arbeiten und ihre Aufgabenfelder regelmäßig wechseln, und in Organisationen die ITIL umsetzen, da hier auch Rollen definiert sind. Wechseln die Mitarbeiter die Aufgaben nicht, sollte die MAC eingesetzt werden.

Das *Access Management,* regelt den autorisierten Zugriff auf Daten, Informationen und Services durch ein Berechtigungskonzept.[256]

Zur Unterstützung des Information Security Managements empfiehlt es sich, zusätzliche Prozesse zu implementieren.[257] Hier sind das Incident Management,[258] das Problem Management,[259] das Release Management,[260] und das Availability Management[261] und das IT-Service Continuity Management[262] von großer Bedeutung.

---

[252] Die Zugriffskontrolle verhindert einen unbefugten Zugriff auf Daten, Geräte und Programme. Vgl. Stahlknecht/Hasenkamp (2005), S. 489.

[253] Bei der RBAC „werden die Zugriffsrechte nicht an Subjekte (beispielsweise Nutzer) sondern an Rollen vergeben." Die Benutzer werden anhand ihrer Aufgaben unterschiedlichen oder gleichen Rollen zugeordnet und erhalten somit die Zugriffsrechte auf Systeme und Daten entsprechend ihrer Rollen. Vorteil dieser Zugriffskontrolle ist deren individuelle Anpassung an die wechselnden Tätigkeiten innerhalb eines Unternehmens. Hansen/Neumann (2005a), S. 311.

[254] Die MAC „ist auf die Steuerung des Informationsflusses ausgelegt. Das Verfahren basiert eine Klassifikation (Einstufung) der Subjekte und Objekte eines Systems." Die Benutzer (Subjekte) sowie die Daten und Programme (Objekte) erhalten zu diesem Zweck eine Sicherheitsmarkierung, mit deren Hilfe der Informationsfluss zwischen Subjekt und Objekt bzw. einem weiteren Subjekt geregelt wird. Die MAC zielt auf eine sichere Datenübertragung zwischen Subjekt und Objekt oder einem zweiten Subjekt ab. Hansen/Neumann (2005a), S. 310 (Hervorhebung im Original).

[255] Vgl. hierzu wie auch für weitere Formen der Zugriffskontrolle Hansen/Neumann (2005a), S. 311.

[256] Vgl. Böttcher (2008), S. 149ff.

[257] Vgl. OGC (2007b), S. 146f.

[258] Das Incident Management dient der schnellen Wiederherstellung von Services, falls diese ausgefallen oder beeinträchtigt sind und nicht mehr in der vereinbarten Qualität zur Verfügung stehen. Da die Störung schnell beseitigt werden soll, ist die Beseitigung der Ursache eines Problems oder Fehlers meist zweitrangig. Vgl. Ebel (2008), S. 65 und Köhler (2005), S. 43.

[259] Die Ursachen von Fehlern werden im Problem Management ergründet, dokumentiert und nachhaltig verbessert, wobei eine nahtlose Schnittstelle zum Incident Management besonders wichtig ist. Ziel ist es durch eine proaktive Fehlererkennung und -behebung Incidents zu verringern. Vgl. Ebel (2008), S. 66; Zarnekow et al. (2005), S. 58; Hofmann (2007), S. 109; OGC (2007b), S. 146f.

[260] Das Release Management hat die Aufgabe unterschiedliche Update-, Patches- und Versionsstände zu dokumentieren, bei Bedarf alte Versionen wiederaufzuspielen bzw. für eine Aktualisierung der Software zu sorgen. Des Weiteren wird die IT-Organisation in einer homogenen Softwarelandschaft in die Lage versetzt, falsche Versionen, illegale Software, Viren und Systemeingriffe effizienter zu entdecken, was die „Stabilität und Zuverlässigkeit des IT-Betriebs" erhöht. Vgl. Köhler (2005), S. 46; Ebel (2008). S. 67; Hofmann (2007), S. 109.

[261] Das Availability Management verfolgt das Ziel, die Verfügbarkeit der IT-Services hinsichtlich der Kundenanforderungen möglichst kostengünstig sicherzustellen, wobei der Verfügbarkeitsgrad aus den SLAs abgeleitet wird. Der Verfügungsgrad wiederum ist von der Zuverlässigkeit, Wartungsfähigkeit und Servicefähigkeit der IT-Infrastruktur abhängig. Vgl. Zarnekow et al. (2005), S. 56f; Sommer (2004), S. 116; Bötcher (2008), S. 53.

[262] Die Implementierung eines IT-Service Continuity Management (ITSCM) sorgt im Falle eines Systemausfalls für dessen Wiederherstellung in einer zuvor festgelegten Zeitspanne und den Anlauf von Überbrückungsmaßnahmen. Bei besonders geschäftskritischen Prozessen und Abläufen ist eine strikte Wiederherstellungs-Regelung vorzunehmen. Weiterhin ist es ratsam, für diese Prozesse eine Business Impact Analyse für eine Festlegung der Minimalanforderungen durchzuführen, um die durch den Ausfall entstehenden Einflüsse auf den Umsatz sowie die Reputation des Unternehmens zu ermitteln. Das ITSCM ist vom Business Continuity Management (BCM) abhängig, da ohne das BCM meist keine Aussagen über die geschäftskritischen Prozesse gemacht werden können. Ohne eine Wiederherstellung der zu unterstützenden Geschäftsprozesse ist die Verfügbarkeit von IT-Services sinnlos. Vgl. Zarnekow et al. (2005), S. 57; Buhl (2008), S. 90.

Das Sicherheitsniveau kann auch durch **physikalische Maßnahmen** gesteigert werden. Hierzu zählen bauliche und infrastrukturelle Veränderungen von Gebäuden, die den Zugang zu Systemen sichern, Systeme vor höherer Gewalt schützen und den Betrieb auch unter schwierigen Bedingungen ermöglichen bis hin zum Einsatz von geeigneten Schutzräumen zur Archivierung von Datenträger und Sicherungskopien.[263]
Zum Schutz vor Unbefugten ist eine Zugangsregelung zu den Systemen zu implementieren, wie spezielle maschinelle Zugangskontrollen der Mitarbeiter über Chipkarten, Geheimnummern oder biometrische Daten. Aber auch eine Implementierung von kompletten Überwachungs- und Schutzsystemen ist anzuraten. Da nicht alle Maßnahmen für jedes Unternehmen sinnvoll sind, sind diese an die gegebenen Umstände und finanziellen Mittel anzupassen.[264]
Ferner sollte eine Identifikation aller internen und externen Mitarbeiter, Besucher und Lieferanten erfolgen, um Sicherheitsvorfälle schneller erkennen zu können.[265]

6.2 Realisierung der ausgewählten Schutzmaßnahmen

Nach der Auswahl der geeigneten Schutzmaßnahmen zur Erhöhung des Sicherheitsniveaus, müssen diese realisiert werden. Hierzu ist eine Tabelle mit den bereits realisierten Maßnahmen aufzustellen, um zu überprüfen, ob nicht einzelne Maßnahmen wegfallen können, da eventuell andere Maßnahmen den gleichen oder einen höheren Schutz bieten. So kann beispielsweise die Passwortabfrage entfallen, wenn auf ein System mit biometrischer Datenerkennung zurückgegriffen wird. Die Eignung der Maßnahmen sollte dahingehend geprüft werden, ob sie einen ausreichenden Schutz vor der Bedrohung bietet und ob sie praktisch umsetzbar ist. Eine Dokumentation der neuen Maßnahmenliste ist hilfreich, um deren Entstehung später nachvollziehen zu können. Für die einzelnen Maßnahmen sind die einmaligen sowie die regelmäßigen personellen und finanziellen Kosten zu ermitteln und seitens des Managements entsprechende Humanressourcen und Budgets für die Implementierung freizugeben. Können relevante Maßnahmen nicht finanziert und realisiert werden, sollten entweder finanzierbare Ersatzmaßnahmen ergriffen werden, die einen ähnlichen Schutzeffekt bieten, oder es muss geprüft werden, ob das Restrisiko selbst tragbar oder versicherbar ist. Ferner ist ein Zeit- und Verantwortlichkeitsplan zu erstellen, um die Maßnahmen in einer bestimmten Zeitspanne fachgerecht realisieren und den Ablauf kontrollieren zu können. Die Mitarbeiter sollten für neue Maßnahmen sensibilisiert sowie in deren Umgang geschult werden, um deren Akzeptanz und Relevanz zu erhöhen.[266]
Auf Grund sich ständig verändernder Rahmenbedingungen, neuer Soft- und Hardware sowie neuen Mitarbeitern und den daraus resultierenden neuen Bedrohungen, reicht die Implementierung von Schutzmaßnahmen alleine zum Erhalt und zur kontinuierlichen Verbesserung der Informationssicherheit nicht aus. Es werden Kontrollen, wie die Erkennung, Dokumentation und Analyse von Sicherheitszwischenfällen benötigt, die den gesamten Informationssicherheitsprozess auf dessen Wirksamkeit und Effizienz überprüfen. Hiermit können neue Fehler und Schwachstellen erkannt werden und demzufolge die Maßnahmen verbessert, erweitert

[263] Vgl. Hofmann (2007a), S. 248 für vertiefende Erläuterungen zu den einzelnen Themen siehe Hoppe/Prieß (2003), S. 247-261.
[264] Vgl. Hansen/Neumann (2005a), S. 313.
[265] Vgl. Brunnstein (2006), S. 112.
[266] Vgl. hierzu BSI (2008a), S. 76-79 und Hofmann (2007a), S. 259f.

oder durch bessere ersetzt werden. Diese gesammelten Daten werden im ISM aufbereitet und ausgewertet, um die Schutzmaßnahmen und die gesamte Informationssicherheit zu steigern. Auch die Sicherheitsziele, die Sicherheitsstrategie und das Sicherheitskonzept sind auf deren Korrektheit und Umsetzbarkeit zu prüfen und an die neuen Veränderungen anzupassen.[267]
Für die Abweichungskontrolle bietet sich ein Sicherheitscheck mittels eines IT-Security Audits an, um Abweichungen von berichteten und vom tatsächlichen IST-Zustand, auf der Basis einer zuvor festgelegten Checkliste, zu ermitteln. Die ermittelten Abweichungen (Findings) sind in einem Audit-Report zu dokumentieren. Der auditierte Bereich sollte zu den Abweichungen aus seiner Sicht Stellung nehmen können und die Gründe hierfür darlegen.[268]
Die Kontrolle dient weiterhin der Überprüfung der Angemessenheit und Wirksamkeit der Schutzmaßnahmen.[269] Wird eine Abweichung festgestellt, so sind die abweichenden Maßnahmen zu verbessern oder durch andere zu ersetzen, um das angestrebte Sicherheitsniveau zu erreichen.

7 Fazit und Ausblick

Die Brisanz des Themas Informationssicherheit und der Einfluss der Menschen auf diese sowie die Abhängigkeit von der IT sind für Unternehmen von großer Bedeutung, denn eine Vernachlässigung der Informationssicherheit kann zu gravierenden Konsequenzen führen.
Die internen Bedrohungen durch den menschlichen Risikofaktor lassen sich verringern, indem die einzelnen Mitarbeiter entsprechend ihres Menschenbildes durch Anreize motiviert werden, sich sicherheitskonform zu verhalten. Ferner gilt, es eine Sinnvermittlung der Sicherheit durch Etablierung einer unternehmensweiten Sicherheitskultur zu schaffen und die Mitarbeiter durch Awareness Kampagnen für die Informationssicherheit zu sensibilisieren. Das adäquate Verhalten und die nötige Qualifikation im Umgang mit der Informationssicherheit können durch Schulungen erlernt und trainiert werden, jedoch können auch bereits vor der Einstellung durch geeignete Verfahren wie AC und Arbeitsproben die Einstellung zur Informationssicherheit geprüft und in Folge dessen sicherheitsbewusste Mitarbeiter rekrutiert werden.
Die Manager sind Teil der Mitarbeiterschaft und müssen ebenso gezielt an die Informationssicherheit durch oben genannte Maßnahmen herangeführt werden, um die Wichtigkeit und die daraus resultierenden Folgen einschätzen zu können. Die Brisanz der Informationssicherheit und aller damit verbunden Konsequenzen müssen von den Managern erkannt werden, damit entsprechende Budgets für Schutzmaßnahmen bereitgestellt werden. Ihre Vorbildfunktion den Mitarbeitern gegenüber können sie nur dann erfüllen, wenn sie selber den sicherheitskonformen Umgang mit den Systemen, Daten und Informationen vorleben, an Schulungen teilnehmen, bei der Erstellung einer Sicherheitskultur aktiv beteiligt sind und die Mitarbeiter situativ führen sowie sie bei ihrer tagtäglichen Arbeit unterstützen.
Es obliegt den Managern, die Budgets für die Schutzmaßnahmen freizugeben, dabei sollte jedoch auf deren Wirtschaftlichkeit geachtet werden. Schon 20% der Schutzmaßnahmen können einen 80%-igen Schutz bieten, wobei jedes weitere Prozent exponentiell ansteigende Kosten verursacht[270] und folglich eine 100%-ige Sicherheit nicht zu realisieren ist.[271]

[267] Vgl. BSI (2008a), S. 82.
[268] Vgl. Schmidt (2007), S. 527.
[269] Vgl. Hofmann (2007a), S. 260.
[270] Vgl. Pohlmann (2006), S. 28f.

Ein effizienter Schutz ist nur durch eine Realisierung von personellen, technischen, prozessualen und physikalischen Maßnahmen in Verbindung mit einem Sicherheitsmanagement, der dazugehörigen Sicherheitspolitik und schriftlich fixierten Sicherheitsrichtlinien zu gewährleisten, um sowohl interne als auch externe Bedrohungen zu minimieren. Eine einseitige Investition in beispielsweise nur technische oder prozessuale Maßnahmen würde das schwächste Glied, den Menschen, nicht berücksichtigen und somit ineffizient sein. Die Wechselwirkungen zwischen den Maßnahmen sind zu berücksichtigen. Nur wenn diese Bedingungen erfüllt sind, kann das Business Continuity durch das richtige Verhalten der Mitarbeiter gewährleisten werden, um finanzielle Schäden aber auch Reputationsschäden zu vermeiden.
Das vorliegende Sicherheitskonzept geht verstärkt auf die personellen Maßnahmen ein, da sie in den Unternehmen stark vernachlässigt werden, obwohl sie die Sicherheit deutlich erhöhen können. Im Rahmen dieser Arbeit ist es jedoch nicht möglich, alle Facetten der möglichen Schutzmaßnahmen zu erörtern. Zudem ist das Konzept noch in der Praxis zu überprüfen.
ITIL als good practice De-facto-Standard vermittelt ein gutes Rüstzeug für die Informationssicherheit, jedoch werden die personellen Maßnahmen nur unzureichend berücksichtigt. Aus diesem Grund wurde das Information-Security Management in ITIL V3 durch das vorgestellte ganzheitliche Sicherheitskonzept bezüglich der personellen und technischen wie aber auch der physikalischen Maßnahmen erweitert und ergänzt. Damit ist ein größerer Schutz vor dem Risikofaktor Mensch gegeben.

Die Bedrohungen der Informationssicherheit werden auch in Zukunft existent sein, wobei sich jedoch die Art ändern kann. Neue Techniken und Verfahren werden auch zukünftig für Bedrohungen sorgen, denen wiederum durch neue technische, prozessuale, physikalische aber auch personelle Maßnahmen zu begegnen ist. Für die Informationssicherheit besteht kontinuierlich Forschungsbedarf, um gegen die Bedrohungen effiziente und kostengünstige oder kostengünstigere Maßnahmen zu entwickeln.
Um die Sicherheitseinstellung der Mitarbeiter zu ermitteln, müssen Verfahren für Interviews, Assessment-Center und Praktika entwickelt werden, die die Validität der Einstellung ermitteln können. Damit könnten Unternehmen in der Lage sein, Mitarbeiter einzustellen, die sich sicherheitskonform verhalten werden und zum Schutz der Informationssicherheit, ihrer Systeme, Daten und Informationen beitragen. Eine Weiterbildungen im Rahmen der Informationssicherheit sollte in regelmäßig erfolgen. Wie solche Schulungen oder Fortbildungen am effizientesten zu gestalten sind, ist noch zu entwickeln.
Die Informationssicherheit darf letztlich nicht in ein Zwangssystem ausarten, welches die Individualität und die Identität der Mitarbeiter ausschließt. Hierzu bedarf es weiterer Forschung, die der Entmenschlichung des Arbeitsplatzes entgegengewirkt, indem z. B. im Rahmen der Unternehmens- und Sicherheitskultur private Dinge auf dem PC zugelassen werden. Dies trägt dazu bei, einem Befreiungsschlag seitens der Mitarbeiter, bei dem sie die Informationssicherheit nicht beachten und Schäden anrichten, entgegen zu wirken.[272]

[271] Vgl. Humpert (2004), S. 16.
[272] Vgl. Pokoyski (2006), S. 1f.

Literaturverzeichnis

Ahrendts, F., Marton, A. (2008) IT-Risikomanagement leben! Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung, Springer Verlag, Berlin/Heidelberg 2008

Baier, H., Buchmann, J., Busch, C. (2003) Aus und Weiterbildung in IT-Sicherheit; in: IT-Sicherheit im verteilten Chaos - Tagungsband 8. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, Ingelheim 2003, S. 179-190

Baier, H., Straub, T. (2005) Awareness by doing – ein neues Konzept zur Sensibilisierung von IT-Anwendern; in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 313-326

Becker, Fred G. (1990) Anreizsysteme für Führungskräfte: Möglichkeiten zur strategisch-orientierten Steuerung des Managements, Poeschel Verlag, Stuttgart 1990

Blickle, Gerhard (2004) Menschenbilder, in: Schreyögg/Werder (Hrsg.), Handwörterbuch Unternehmensführung und Organistaion, 4., völlig neu überarbeitete Auflage, Schäffer-Pöschel Verlag, Stuttgart 2004, Sp. 836-843

Bock, W., Macek, G., Oberndorfer, T., Pumsenberger, R. (2008) Praxisbuch ITIL: Erfolgreiche Zertifizierung nach ISO 20000, 2. aktuelle und erweiterte Auflage, Galileo Press, Bonn 2008

Böttcher, Roland (2008) IT-Servicemanagement mit ITIL® V3: Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen, 1. Auflage, Heise Verlag, Hannover 2008

Bon, Jan von (2008) IT-Service Management basierend auf ITIL V3 - Das Taschenbuch, itSMF Inernational, 1. Auflage, Van Haren Publishing, Zaltbommel 2008

Bruch, Heike (1996) Intra- und interorganisationale Delegation als Managementaufgabe: Entwicklung eines markt-, potential- und wertorientierten Modells, Dissertation; Universität Hannover, 1996

Brunnstein, Jochen (2006) ITIL Security Management realisieren: IT-Service Security Management nach ITIL – So gehen Sie vor, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2006

Buchsein, R., Victor, F., Günther, H., Machmeier, V. (2008) IT-Management mit ITIL® V3: Strategien, Kennzahlen, Umsetzung; 2., aktualisierte und erweiterte Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Buhl, Ulrike (2008) ITIL Praxisbuch: Beispiele und Tipps für die erfolgreiche Prozessoptimierung, 2. Auflage, mitp Redline GmbH, Heidelberg 2008

Buerschaper, Cornelius (2008) Organisationen - Kommunikationssystem und Sicherheit, in: Badke-Schaub, P./Hofinger, G./Lauche, K. (Hrsg.), Human Factors: Psychologie sicheren Handelns in Risikobranchen, Springer Verlag, Berlin/Heidelberg 2008, S. 155-175

BSI (2005) IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005

Deci, E. L., Ryan, R. M. (1993) Die Selbstbestimmungstheorie und der Motivation und ihre Bedeutung für die Pädagogik, in: Zeitschrift für Pädagogik, 39. Jg. 1993 Nr. 2, S. 223-238

Drumm, Hans-Jürgen (2008) Personalwirtschaft, 6., überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2008

Ebel, Nadin (2008) ITIL® Basis-Zertifizierung: Grundlagen und Zertifizierungsvorbereitung für die ITIL® Foundation-Prüfung, Addison-Wesley-Verlag, München 2008

Eckert, Claudia (2008) IT-Sicherheit: Konzepte – Verfahren – Protokolle, 5., überarbeitete Auflage, Oldenbourg Verlag, München 2008

Engelkamp, P., Sell, F. L. (2005) Einführung in die Volkswirtschaftslehre, 3., verbesserte Auflage, Springer Verlag, Berlin Heidelberg 2005

Eschweiler, J., Psille, D. (2006) Security@Work: Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open Source Basis, Springer Verlag, Berlin/Heidelberg 2006

Falke, Ulrich (2003) Scheinbar sicher- Eine Zusammenfassung von Ergebnissen aktueller Befragungen und Expertengespräche, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 181-196

Fox, Dirk (2003) Security Awareness oder: Die Wiederentdeckung des Menschen in der IT-Sicherheit; in: Datenschutz und Datensicherheit 27 (2003) 11, 2003, S. 676-680

Fox, D., Kaun, S. (2005) Security Awareness Kampagnen, in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 329-337

Friberg, C., Gerhardt, C, Luttenberger, N. (2003) Die Integration von Schutzbedarfsanalysen und IT-Grundschutz nach BSI, in: Gora, W./ Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 65-79

Gabriel, Roland (2006) IT-Sicherheit und Data Warehousing; in: Chamoni, P./Gluchowski, P. (Hrsg.), Analytische Informationssysteme: Business Intelligence-Technologie und -Anwendungen, dritte, vollständig überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2006, S. 439-450

Geiger, Gebhard (2007) IT-Sicherheit als integraler Bestandteil des Risikomanagements im Unternehmen, in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 27-51

Gründer, Torsten (2007) IT-Controlling mit Service Level Agreements SLA Performance Cycle (SLAPeC), in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 235-247

Hansen, H. R., Neumann G. (2005a) Wirtschaftsinformatik 1: Grundlagen und Anwendungen, 9. Auflage, Lucius & Lucius Verlagsgesellschaft mbH, Stuttgart 2005

Hansen, H. R., Neumann G. (2005b) Wirtschaftsinformatik 2: Informationstechnik, 9. Auflage, Lucius & Lucius Verlagsgesellschaft mbH, Stuttgart 2005

Heinrich, L. J., Heinzl, A., Roithmeyer, F. (2007) Wirtschaftsinformatik: Einführung und Grundlegung, dritte, vollständig überarbeitete und ergänzte Auflage, Oldenbourg Verlag, München 2007

Hentze, J., Graf. A., Kammel, A., Lindert, K. (2005) Personalführungslehre: Grundlagen, Funktionen und Modelle der Führung, 4., neu bearbeitete Auflage, Haupt Verlag, Berlin/Stuttgart/Wien 2005

Hersey, P., Blanchard, K. (1982) Management of Organizational Behaviour: Utilizing Human Resources, fourth edition, Prentice Hall, London et al., 1982

Hesch, Gerhard (1997) Das Menschenbild neuer Organisationsformen: Mitarbeiter und Manager im Unternehmen der Zukunft, Gabler Verlag, Wiesbaden 1997

Hofmann, Jürgen (2007) IT-Organisation und Personal, in: Hofmann, J./Schmidt, W. (Hrsg.), Masterkurs IT-Management: Das Wissen für die erfolgreiche Praxis - Grundlagen und beispielhafte Umsetzung - Für Studenten und Praktiker, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2007, S. 91-140

Hofmann, Jürgen (2007a) IT-Sicherheitsmanagement, in: Hofmann, J./Schmidt, W. (Hrsg.), Masterkurs IT-Management: Das Wissen für die erfolgreiche Praxis - Grundlagen und beispielhafte Umsetzung - Für Studenten und Praktiker, 1. Auflage, Vieweg & Sohn Verlag, Wiesbaden 2007, S. 233-274

Holey, T., Welter, G., Wiedemann, A. (2004) Wirtschaftsinformatik, Friedrich Kiehl Verlag, Ludwigshafen (Rhein) 2004

Hoppe, G., Prieß, A. (2003) Sicherheit von Informationssystemen: Gefahren, Maßnahmen und Management im IT-Bereich, nwb Verlag, Herne/Berlin 2003

Humpert, Frederik (2004) IT-Sicherheit, in: HMD Praxis der Wirtschaftsinformatik 236, 2004, S. 7-18

Hungenberg, H., Wulf, T. (2007) Grundlagen der Unternehmensführung, 3., aktualisierte und erweiterte Auflage, Springer Verlag, Berlin Heidelberg, New York 2007

Jung, Hans (2006) Personalwirtschaft, 7., überarbeitete Auflage, Oldenbourg Verlag, München 2006

Kirchler, E., Meier-Pesti, K., Hofmann, E. (2004) Menschenbilder in Organisationen, WUV - Universitätsverlag, Wien 2004

Köhler, R.-D., Krampert,T., van Hülsen, E. (2003) Von der IT-Sicherheitsanforderung zum Service Level Agreement, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 333-352

Kopperger, D., Kunsmann, J., Weisbecker, A. (2007) IT-Servicemanagement, in: Tiemeyer, E. (Hrsg.), Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, Carl Hanser Verlag, München/ Wien 2007, S. 121-257

Krcmar, Helmut (2005) Informationsmanagement, 4., überarbeitete und erweiterte Auflage, Springer Verlag, Berlin/Heidelberg, 2005

Lardschneider, Martin (2008) Social Engineering: Eine ungewöhnliche aber höchst effiziente Security Awareness Maßnahme; in: Datenschutz und Datensicherheit (DuD), 09/2008, S. 574-578

Lassmann, Wolfgang (2006) Kapitel 9 IT-Sicherheit in; Lassmann, W. (Hrsg.): Wirtschaftsinformatik Nachschlagewerk für Studium und Praxis; 1. Auflage, Gabler Verlag, Wiesbaden 2006 S. 349-408

Lehner, F., Wildner, S., Scholz, M. (2007)Wirtschaftsinformatik: Eine Einführung, Carl Hanser Verlag, München/Wien, 2007

Matthiesen, Kai H. (1995) Kritik des Menschenbildes in der Betriebswirtschaftslehre: Auf dem Weg zu einer sozialökonomischen Betriebswirtschaftslehre, Haupt Verlag, Bern/Stuttgart/Wien 1995

Mertens, P., Bodendorf, F., König, W., Picot, A., Schumann, M. (2001) Grundzüge der Wirtschaftsinformatik, 7., neu bearbeitete Auflage, Springer Verlag, Berlin/Heidelberg/New York, 2001

Mix, M., Pingel, M. (2007) Be Better – Be Sure: Security Awareness in der Bosch Gruppe; in: Datenschutz und Datensicherheit (DuD) 31 (2007) 7, 2007, S. 498-501

Müller, Klaus-Rainer (2005) IT-Sicherheit mit System: Sicherheitspyramide und Vorgehensmodelle - Sicherheitsprozess und Katastrophenvorsorge – Die 10 Schritte zum Sicherheitsmanagement, 2., verbesserte und aktualisierte Auflage, Vieweg und Sohn Verlag, Wiesbaden 2005

Münch, Isabel (2007) IT-Grundschutz zum Bewältigen von IT-Risiken in Unternehmen; in: Gründer, T./Schrey, J. (Hrsg.), Managementhandbuch IT-Sicherheit: Risiken, Basel II, Recht, Erich Schmidt Verlag, Berlin 2007, S. 285-308

Neuberger, Oswald (2002) Führen und führen lassen: Ansätze, Ergebnisse und Kritik der Führungsforschung, 6., völlig neu bearbeitete und erweiterte Auflage, Lucius & Lucius Verlag, Stuttgart 2002

Oechsler, Walter (2005) Personal und Arbeit: Grundlagen des Human Resource Management und der Arbeitgeber-Arbeitnehmer-Beziehung, 8., grundlegend überarbeitete Auflage, Oldenbourg Verlag, München Wien 2005

OGC (2007a) Office of Government Commerce (OCG) (Hrsg.): ITIL Service Strategy, TSO (The Stationery Office), Crown Copyright, London 2007

OGC (2007b) Office of Government Commerce (OCG) (Hrsg.): ITIL Service Design, TSO (The Stationery Office), Crown Copyright, London 2007

Olbrich, Alfred (2008) ITIL kompakt und verständlich erklärt: Effizientes IT-Management – Den Standard für IT-Prozesse kennenlernen, verstehen und erfolgreich in der Praxis umsetzen, 4., erweiterte und verbesserte Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Poguntke, Werner (2007) Basiswissen IT-Sicherheit: Das Wichtigste für den Schutz von Systemen & Daten, W3L-Verlag, Herdecke/Witten 2007

Pohl, Lorenz (2007) 2. Kapitel: Datenschutzrecht, Teil I: Rechtliche Aspekte der IT-Sicherheit; in: Reinhard/Pohl/Capellaro (Hrsg.), IT-Sicherheit und Recht: Rechtliche und technisch-organisatorische Aspekte für Unternehmen, Schmidt Verlag, Berlin 2007, S. 55-93

Pohlmann, Norbert (2003) Firewall-Systeme, 5. aktualisierte Auflage, mitp-Verlag, Bonn 2003

Pohlmann, Norbert (2006) Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?, in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 26-34

Pohlmann, Norbert (2008) Herausforderung Compliance, in: Pohlmann, Norbert (Hrsg.), Organisationshandbuch Netzwerksicherheit: Praxislösungen für den Netzwerkverantwortlichen Band 1, Weka Medien GmbH& Co. KG, Kissingen 2008, Teil2/6.2, S. 1-8

Pohlmann, N., Blumberg, H. (2006) Der IT-Sicherheitsleitfaden: Das Pflichtheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen, 2., aktualisierte Auflage, mitp-Verlag, Heidelberg 2006

Prottung, Stefan (2008) Auf dem Weg zur Geschäftsentwicklung mit der IT – Die innovative Kraft der IT für die Geschäftsentwicklung nutzen, in: Keuper F. /Schomann, M./ Grimm, R. (Hrsg.), Strategisches IT-Management: Management von IT und IT-gestütztes Management, 1. Auflage, Gabler / GWV Fachverlage GmbH, Wiesbaden 2008, S. 63-78

Raepple, Martin (2001) Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, 2. überarbeitete und erweiterte Auflage, dpunkt Verlag, Heidelberg 2001

Rauschen, T., Disterer, G. (2004) Identifikation und Analyse von Risiken im IT-Bereich, in: HMD Praxis der Wirtschaftsinformatik 236, 2004, S. 19-32

Reichenbach, Martin (2004) Sicherheitsmanagement und Versicherungsmöglichkeit, in: Ernst, Stefan (Hrsg.); Hacker, Cracker & Computerviren: Recht und Praxis der Informationssicherheit, OVS Verlag Dr. Otto Schmidt, Köln 2004, S. 329-353

Reinhard, Tim (2007) 1. Kapitel: Grundlagen; Teil I: Rechtliche Aspekte der IT-Sicherheit; in: Reinhard/Pohl/Capellaro (Hrsg.), IT-Sicherheit und Recht: Rechtliche und technisch-organisatorische Aspekte für Unternehmen, Schmidt Verlag, Berlin 2007, S. 37-47

Ridder, Hans-Gerd (2007) Personalwirtschaftslehre, 2., überarbeitete Auflage, Verlag W. Kohlhammer, Stuttgart 2007

Rosenstiel, Lutz von (1975) Die motivationalen Grundlagen des Verhaltens in Organisationen – Leistung und Zufriedenheit, Duncker & Humblot Verlag; Berlin 1975

Rotenstrauch, C., Schulze, T. (2003) Informatik für Wirtschaftswissenschaftler und Wirtschaftsinformatiker, Springer Verlag, Heidelberg/Berlin 2003

Schadt, Dirk (2006) Über die Ökonomie der IT-Sicherheit: Betrachtungen zum Thema »Return on Security Investment«, in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 16-25

Schein, Edgar H. (1980) Organizational Psychology, 3rd edition, Prentice-Hall International, London 1980; deutsche Version: Organisationspsychologie, Gabler Verlag, Wiesbaden 1980

Schimmer, Klaus (2007) Sicherheit beginnt im Kopf: Sensibilisieren - aber wie?, in: Datenschutz und Datensicherheit 31 (2007) 7, 2007, S. 510-514

Schlienger, Thomas (2003) Sicherheitskultur: der Mensch in der Informationssicherheit, in: Switchjournal 1/2003, S. 34-37

Schlienger, T., Baur, C., Barau, S. et al. (2004) Leitfaden zur Förderung und Analyse der Informationssicherheitskultur: Abschlussbereicht der Arbeitsgruppe „Informationssicherheitskultur“ der FGSec fachlichen Sektion der Schweizer Informatik Gesellschaft, iimt University Press, Fribourg 2004

Schlienger, Thomas (2007) Informationskultur: Messung, Planung, Steuerung; in: Datenschutz und Datensicherheit (DuD) 31 (2007) 7, 2007, S. 487-491

Scholz, Christian (1994) Personalmanagement: Informationsorientierte und verhaltenstheoretische Grundlagen, 4., verbesserte Auflage, Franz Vahlen Verlag, München 1994

Scholz, Christian (2000) Personalmanagement: Informationsorientierte und verhaltenstheoretische Grundlagen, 5., neubearbeitete und erweiterte Auflage, Franz Vahlen Verlag, München 2000

Schreiber, Sebastian (2006) Kosten und Nutzen von Penetrationstest**,** in: HMD Praxis der Wirtschaftsinformatik 248, 2006, S. 86-91

Schultz, Eugene (2005) The human factor in security; in: Computers & Security (2005) 24, p. 425-426

Schwyter, F., Wisler, A. (2007) Informationssicherheit für KMU: Sicherheitskonzepte & praktische Umsetzung, BPX-Edition, Rheinfelden (Schweiz) 2007

Seibold, Holger (2006) IT-Risikomanagement, Oldenbourg Verlag, München Wien 2006

Solms, von / von Solms (2004) The 10 deadly sins of information security management; in: Computer & Security (2004) 23, p. 371-376

Sommer, Jochen (2004) IT-Servicemanagement mit ITIL® und MOF, 1. Auflage, mitp Verlag, Bonn 2004

Spector, Paul E. (1996) Industrial and organizational psychology: research and practice, John Wiley & Sons, New York [u. a.] 1996

Staehle, Wolfgang H. (1999) Management: Eine verhaltenswissenschaftliche Perspektive, 8. Auflage überarbeitet von Conrad, P. und Sydow, J., Verlag Franz Vahlen, München 1999

Stahlknecht, P., Hasenkamp, U. (2005) Einführung in die Wirtschaftsinformatik, elfte, vollständig überarbeitete Auflage, Springer Verlag, Berlin/Heidelberg 2005

Steinle, Claus (1978) Führung: Grundlagen, Prozesse und Modelle der Führung in der Unternehmung, C. E. Poeschel Verlag, Stuttgart 1978

Steinle, C., Ahlers, F. (2004) Menschenbilder, in: Gaugler, E./Oechsler, W./Weber, W. (Hrsg.), Handwörterbuch des Personalwesens, 3., überarbeitete und ergänzte Auflage, Schäffer-Poeschel Verlag, Stuttgart 2004, Sp. 1142-1151

Steinle, Claus (2007) Unternehmensführung – ein »grundlegender« Überblick; in: Steinle, C./Daum, A. (Hrsg.), Controlling: Kompendium für Ausbildung und Praxis, 4., überarbeitete Auflage, Schäffer-Poeschel Verlag, Stuttgart 2007

Suter, W. (1999) Motivation; in: Steiger, Th./Lippmann, E. (Hrsg.): Handbuch angewandte Psychologie für Führungskräfte: Führungskompetenz und Führungswissen, Springer Verlag, Berlin /Heidelberg 1999, S. 132-142

Swoboda, J., Spitz, S., Pramateftakis, M. (2008) Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen, 1. Auflage, Vieweg + Teubner Verlag, Wiesbaden 2008

Temme, Matthias (2004) (Un)-Sicherheitspotenzial Mitarbeiter, in: <kes> Die Zeitschrift für Informationssicherheit, Nr. 2, März 2004, S. 10-14

Töpfer, Armin (2005) Betriebswirtschaftslehre: Anwendungs- und prozessorientierte Grundlagen, Springer Verlag, Berlin/Heidelberg 2005

Tsintsifa, Lydia (2005) IT-Sicherheitskultur mit IT-Grundschutz, in: IT-Sicherheit geht alle an! – Tagungsband zum 9. Deutschen IT-Sicherheitskongress, SecuMedia Verlag, Ingelheim 2005, S. 219-228

Ulrich, Hans (1990) Unternehmenspolitik, 3. Auflage, Haupt Verlag, Bern, Stuttgart 1990

Uth, S., Demon, S., Petrov, W. (2008) Sicherheit an öffentlichen Computerarbeitsplätzen des CMS, in: cms-journal 30, Juni 2008, S. 38-41

Weinert, Ansfried B. (1995) Menschenbilder und Führung, in: Kieser (Hrsg.), Handwörterbuch der Führung, 2., neu gestaltete Auflage, Schäffer-Pöschel Verlag, Stuttgart 1995, Sp. 1495-1510

Weinert, Ansfried B. (2004) Organisations- und Personalpsychologie, 5., vollständig, überarbeitete Auflage, Beltz Verlag, Basel 2004

Wiltner, Frank (2003) Bedrohungen für Unternehmen, in: Gora, W./Krampert, T. (Hrsg.), Handbuch IT-Sicherheit: Strategien, Grundlagen und Projekte, Addison-Wesley-Verlag, München 2003, S. 81-96

Wunderer, Rolf (2007) Führung und Zusammenarbeit: Eine unternehmerische Führungslehre, 7., überarbeitete Auflage, Luchterhand Verlag, München 2007

Zarnekow, R./Brenner, W./Pilgrim, U. (2005) Integriertes Informationsmanagement: Strategien und Lösungen für das Management von IT-Dienstleistungen, Springer Verlag, Berlin/Heidelberg 2005

Zerr, Konrad (2007) Security-Awareness-Monitoring: Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewußtseins bei Mitarbeitern: in: Datenschutz und Datensicherheit 31 (2007) 7, 2007, S. 519-523

Onlinequellen:

Abawajy, J. H., Thatcher, K., Kim, T. (2008) Investigation of Stakeholders Commitment to Information Security Awareness Programs, in: International Conference on Information Security Assurance, p. 472-476, online unter: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4511613&isnumber=4511515 [13.01.2009]

Bitkom (o. J.) Sicherheit für Systeme und Netze in Unternehmen: Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, 2. überarbeitete Auflage, online unter: http://www.bitkom.org/de/themen_gremien/54746_38229.aspx [24.12.2008]

BSI (2007) Leitfaden IT-Sicherheit: IT-Grundschutz kompakt, unter : http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf [02.12.08]

BSI (2008a) BSI Standard 100-2: IT-Grundschutz-Vorgehensweise Version 2, unter http://www.bsi.bund.de/literat/bsi_standard/standard_1002.pdf [23.12.2008]

Deloitte (2007) 2007 Global Security Survey – The shifting security paradigm, 2007 unter http://www.deloitte.org/dtt/cda/doc/content/us_fsi-DeloitteGlobalSecuritySurvey2007.pdf [26.01.2009]

Dolya, Alexey (2007a) Interne IT-Bedrohung in Europa 2006, Infowatch, online unter: http://www.infowatch.com/de/threats?ipcountry=DE&chapter=162971949&id=26#it [20.11.08]

ohne Verfasser (2008) Lagebericht zur Informations-Sicherheit 1, in: <kes> Die Zeitschrift für Informationssicherheit, Nr.4, August 2008, online unter: http://www.kes.info/archiv/heft/abonnent/08-4/08-4-018.htm [28.01.2009]

Oltmann, Uwe (2008) Der VPN-Dienst an der Universität Hannover, online unter: http://www.rrzn.uni-hannover.de/index.php?id=141&no_cache=1&type=98 [21.01.09]

Pokoyski, Dietmar (2006) Entsicherung am Arbeitsplatz – Studie entschlüsselt erstmalig psychologische Wirkweisen und Zusammenhänge der IT-Security, online unter: http://www.securitymanager.de/magazin/artikel_1184-print_entsicherung_am_arbeitsplatz_studie.html [16.12.08]

Topf, Jochen (2005) Antispam-Strategien: Unerwünschte E-Mails erkennen und abwehren, Bundesamt für Sicherheit in der Informationstechnik, Bundesanzeiger, Köln 2005, online unter: http://www.bsi.bund.de/literat/studien/antispam/antispam.pdf [19.11.08]

Wieshoff, Rainer (2005) USB-Sperre: Übertriebenes Misstrauen oder legitime Vorsicht? unter: http://www.channelpartner.de/knowledgecenter/security/grundlagen/200997/ [03.12.08]

Wiedemann, Jochen (2007)

Gestaltung von IT-Notfallvorsorge im Kontext des Risikomanagements Teil2: Entwicklung von Gestaltungselementen am Beipiel einer TK-Unternehmung, Institut für Sicherheit im E-Business (ISEB), Nr. 27, unter http://www.iseb.ruhr-uni-bochum.de/download/ISEB-AB-27-Wiedemann_2.pdf, [17.11.08]

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Michael H. Breitner, *Rufus Philip Isaacs and the Early Years of Differential Games*, 36 p., #1, January 22, 2003.

Gabriela Hoppe and Michael H. Breitner, *Classification and Sustainability Analysis of e-Learning Applications*, 26 p., #2, February 13, 2003.

Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 S., #3, 14. Februar, 2003.

Patrick Bartels and Michael H. Breitner, *Automatic Extraction of Derivative Prices from Webpages using a Software Agent,* 32 p., #4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, *WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options,* 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe und Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 S., #6, 21. Oktober, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann und Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 S., #8, 21. Juni, 2004.

Dennis Bode und Michael H. Breitner, *Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte,* 21 S., #9, 5. Juli, 2004.

Caroline Neufert und Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 S., #10, 5. Juli, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 22 p., #11, July 5, 2004.

Liina Stotz, Gabriela Hoppe und Michael H. Breitner, *Interaktives Mobile(M)-Learning auf kleinen End-geräten wie PDAs und Smartphones*, 31 S., #12, 18. August, 2004.

Frank Köller und Michael H. Breitner, *Optimierung von Warteschlangensystemen in Call Centern auf Basis von Kennzahlenapproximationen,* 24 S., #13, 10. Januar, 2005.

Phillip Maske, Patrick Bartels and Michael H. Breitner, *Interactive M(obile)-Learning with UbiLearn 0.2*, 21 p., #14, April 20, 2005.

Robert Pomes and Michael H. Breitner, *Strategic Management of Information Security in State-run Organizations,* 18 p., #15, May 5, 2005.

Simon König, Frank Köller and Michael H. Breitner, *FAUN 1.1 User Manual,* 134 p., #16, August 4, 2005.

Christian von Spreckelsen, Patrick Bartels und Michael H. Breitner, *Geschäftsprozessorientierte Analyse und Bewertung der Potentiale des Nomadic Computing,* 38 S., #17, 14. Dezember, 2006.

Stefan Hoyer, Robert Pomes, Günter Wohlers und Michael H. Breitner, *Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT) am Beispiel CERT-Niedersachsen,* 56 S., #18, 14. Dezember, 2006.

Christian Zietz, Karsten Sohns und Michael H. Breitner, *Konvergenz von Lern-, Wissens- und Personalmanagementssystemen: Anforderungen an Instrumente für integrierte Systeme,* 15 S., #19, 14. Dezember, 2006.

Christian Zietz und Michael H. Breitner, *Expertenbefragung „Portalbasiertes Wissensmanagement": Ausgewählte Ergebnisse*, 30 S., #20, 5. Februar, 2008.

IWI Discussion Paper Series/Diskussionsbeiträge

ISSN 1612-3646

Harald Schömburg und Michael H. Breitner, *Elektronische Rechnungsstellung: Prozesse, Einsparpotentiale und kritische Erfolgsfaktoren*, 36 S., #21, 5. Februar, 2008.

Halyna Zakhariya, Frank Köller und Michael H. Breitner, *Personaleinsatzplanung im Echtzeitbetrieb in Call Centern mit Künstlichen Neuronalen Netzen*, 35 S., #22, 5. Februar, 2008.

Jörg Uffen, Robert Pomes, Claudia M. König und Michael H. Breitner, *Entwicklung von Security Awareness Konzepten unter Berücksichtigung ausgewählter Menschenbilder*, 14 S., #23, 5. Mai, 2008.

Johanna Mählmann, Michael H. Breitner und Klaus-Werner Hartmann, *Konzept eines Centers der Informationslogistik im Kontext der Industrialisierung von Finanzdienstleistungen*, 19 S., #24, 5. Mai, 2008.

Jon Sprenger, Christian Zietz und Michael H. Breitner, *Kritische Erfolgsfaktoren für die Einführung und Nutzung von Portalen zum Wissensmanagement*, 44 S., #25, 20. August, 2008.

Finn Breuer und Michael H. Breitner, *„Aufzeichnung und Podcasting akademischer Veranstaltungen in der Region D-A-CH": Ausgewählte Ergebnisse und Benchmark einer Expertenbefragung*, 30 S., #26, 21. August, 2008.

Harald Schömburg, Gerrit Hoppen und Michael H. Breitner, *Expertenbefragung zur Rechnungseingangsbearbeitung: Status quo und Akzeptanz der elektronischen Rechnung*, 40 S., #27, 15. Oktober, 2008.

Hans-Jörg von Mettenheim, Matthias Paul und Michael H. Breitner, *Akzeptanz von Sicherheitsmaßnahmen: Modellierung, Numerische Simulation und Optimierung,* 30 S., #28, 16. Oktober, 2008.

Markus Neumann, Bernd Hohler und Michael H. Breitner, *Bestimmung der IT-Effektivität und IT-Effizienz serviceorientierten IT-Managements,* 20 S., #29, 30. November, 2008.

Matthias Kehlenbeck und Michael H. Breitner, *Strukturierte Literaturrecherche und -klassifizierung zu den Forschungsgebieten Business Intelligence und Data Warehousing,* 10 S., #30, 19. Dezember, 2009.

Michael H. Breitner, Matthias Kehlenbeck, Marc Klages, Harald Schömburg, Jon Sprenger, Jos Töller und Halyna Zakhariya, *Aspekte der Wirtschaftsinformatikforschung 2008,* 128 S., #31, 12. Februar, 2009.

Sebastian Schmidt, Hans-Jörg v. Mettenheim und Michael H. Breitner, *Entwicklung des Hannoveraner Referenzmodels für Sicherheit und Evaluation an Fallbeispielen,* 30 S., #32, 18. Februar, 2009.

Sissi Eklu-Natey, Karsten Sohns und Michael H. Breitner, *Buildung-up Human Capital in Senegal - E-Learning for School drop-outs, Possibilities of Lifelong Learning Vision,* 39 S., #33, July 1, 2009.

Horst-Oliver Hofmann, Hans-Jörg von Mettenheim und Michael H. Breitner, *Prognose und Handel von Derivaten auf Strom mit Künstlichen Neuronalen Netzen,* 34 S., #34, 11. September, 2009.

Christoph Polus, Hans-Jörg von Mettenheim und Michael H. Breitner, *Prognose und Handel von Öl-Future-Spreads durch Multi-Layer-Perceptrons und High-Order-Neuronalnetze mit Faun 1.1 ,* 55 S., #35, 18. September, 2009.

Jörg Uffen und Michael H. Breitner, *Stärkung des IT-Sicherheitsbewusstseins unter Berücksichtigung psychologischer und pädagogischer Merkmale*, 37 S., #36, 24. Oktober, 2009.

Christian Fischer und Michael H. Breitner, *MaschinenMenschen – reine Science Fiction oder bald Realität?,* 36 S., #37, 13. Dezember, 2009.

Tim Rickenberg, Hans-Jörg von Mettenheim und Michael H. Breitner, *Plattformunabhängiges Softwareengineering eines Transportmodells zur ganzheitlichen Disposition von Strecken- und Flächenverkehren,* 38 S., #38, 11. Januar, 2010.