


*Ein ganzheitliches Konzept für Informationssicherheit
unter besonderer Berücksichtigung des Schwachpunktes
Mensch*

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von:

Björn Semmelhaack



Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, 03. Februar 2009

Abbildungsverzeichnis	III
Tabellenverzeichnis	III
Abkürzungsverzeichnis.....	IV
1 Notwendigkeit der Informationssicherheit in einem Unternehmen	1
1.1 Motivation	1
1.2 Vorgehensweise der Arbeit	2
2 Grundanforderungen an die Informationssicherheit	4
2.1 Definitionen und rechtliche Grundlagen	4
2.2 IT-Sicherheitsziele	7
2.3 IT-Sicherheitsstrategie	8
2.4 IT-Sicherheit als Service	10
2.4.1 IT-Service Management	10
2.4.2 Notwendigkeit von Service Level Agreements.....	11
2.5 Outsourcing als Variante einer Dienstleistungsvergabe.....	13
3 Bedrohungen der Informationssicherheit und Investitionen in Schutzmaßnahmen 16	16
3.1 IT-Abhängigkeiten	16
3.2 Mögliche Gefahrenpotentiale und ihre Wirkung auf die IT	18
3.2.1 Externe Bedrohungen	22
3.2.2 Interne Bedrohungen	25
3.3 Schadenshöhen und Eintrittswahrscheinlichkeiten	27
3.4 „Value of IT“: die Investitionen in die Informationssicherheit.....	29
4 Komponenten und Akteure in der Informationssicherheit.....	35
4.1 Hardwarekomponenten	35
4.2 Softwarekomponenten.....	36
4.3 Akteure in der Informationssicherheit.....	37
4.4 Unterschiedliche Menschenbilder der Akteure	42
4.4.1 Definition Menschenbilder.....	42
4.4.2 Dualistisches Menschenbild nach McGregor.....	43
4.4.3 Menschenbildtypologie nach Edgar E. Schein.....	45
5 Konzept zur Informationssicherheit in ITIL V3 unter Berücksichtigung der unterschiedlichen Menschen in einer Organisation und deren Motivation.....	49
5.1 Definitive Abgrenzung der Begriffe Sicherheitspolitik und ganzheitliches Sicherheitskonzept	49
5.2 Ableitung einer Sicherheitskultur aus der Unternehmenskultur	50
5.3 ITIL V3	53
5.3.1 Was ist ITIL V3?.....	53
5.3.2 Information Security Management in ITIL V3	54
5.3.2.1 Information Security Management System.....	55
5.3.2.2 Informationssicherheitspolitik.....	57
5.3.2.3 Prozessaktivitäten, Methoden und Techniken.....	58
5.3.2.4 Sicherheitskontrollen in ITIL V3	58
5.3.2.5 Fehlende Aspekte in ITIL V3.....	60

5.4	Erstellung eines ganzheitlichen Sicherheitskonzeptes	61
5.4.1	Strukturanalyse	62
5.4.2	Schutzbedarfsermittlung	63
5.4.3	Maßnahmenplanung	65
5.4.4	Personelle Maßnahmen	65
5.4.4.1	Motivation, Anreize und Rekrutierung der Mitarbeiter	66
5.4.4.2	Anwendung eines adäquaten Führungsstils	70
5.4.4.3	Aufgaben des Managements und Unterstützung durch das Management	72
5.4.4.4	Qualifikation der Mitarbeiter durch Schulungen	74
5.4.4.5	Security Awareness Kampagnen	75
5.4.5	Technische Maßnahmen	78
5.4.5.1	Antiviren-Software	78
5.4.5.2	Firewalls	78
5.4.5.3	Intrusion Detection Systeme	79
5.4.5.4	Sicherung von LAN- und WLAN-Verbindungen	80
5.4.5.5	Redundanz der Systeme und Daten	81
5.4.5.6	Kontinuierliche Datenbackups	82
5.4.5.7	Erfordernis regelmäßiger Updates und Patches der Software	83
5.4.6	Prozessuale Maßnahmen und physikalische Maßnahmen	84
5.4.6.1	Rollen und Berechtigungen	85
5.4.6.2	Prozessuale Maßnahmen in ITIL V3	86
5.4.6.3	Bauliche Maßnahmen	88
5.4.7	Realisierung der ausgewählten Schutzmaßnahmen	88
5.4.8	Sicherheitskontrollen	89
6	Fazit und Ausblick	90
6.1	Fazit	90
6.2	Ausblick	92
	Literaturverzeichnis	93
	Verzeichnis der Anhänge	109
	Anhang	110

1 Notwendigkeit der Informationssicherheit in einem Unternehmen

1.1 Motivation

Dass Informationen und Daten ein extrem sensibler Faktor eines Unternehmens sind, die es durch geeignete Mittel zu schützen gilt, hat aktuell das Negativbeispiel der Telekom AG und ihrer Tochtergesellschaft T-Mobile gezeigt, denen insgesamt 17 Millionen Kundendaten gestohlen wurden.¹ Zudem war der Zugang zum Kundensystem nicht ordentlich gesichert, so dass leicht in das System eingedrungen und die Daten manipuliert werden konnten.² Leider wird der Schutz bzw. die Implementation von Schutzmaßnahmen der Informationstechnik (IT) in vielen Unternehmen vernachlässigt.³

Im Wandel von der Industriegesellschaft zur Informationsgesellschaft und der damit verbundenen Fülle an Daten und Informationen⁴, die erstellt, verarbeitet, gespeichert und wieder gelöscht werden, bedarf es einer adäquaten Informationssicherheit. Die Informationssicherheit soll dafür Sorge tragen, dass Informationen jeder Zeit verfügbar sind, jedoch nur für autorisierte Stellen. Die Informationssicherheit besteht zum einen aus der IT-Sicherheit, d. h. aus Informationen innerhalb eines Unternehmens (Informationsschutz) sowie deren Datenbestände (Datenschutz) und zum anderen aus dem Schutz der IT-Technik, welche in Unternehmen genutzt werden, um Umsätze generieren zu können. Dabei werden meist sämtliche Geschäftsprozesse durch die IT unterstützt⁵ und somit bildet sie das Rückgrat fast jedes Unternehmens, Behörde oder sonstigen Einrichtungen.⁶ Falls Systeme versagen oder Datenverluste auftreten, kann dies weit reichende Folgen für einen Betrieb oder eine Behörde haben, wie z. B. Industriespionage, die Neuerfassung von Daten, den Wiederanlauf von Produktionsstätten und damit verbundene Kosten oder Umsatzeinbußen bis hin zu lebensbedrohlichen Situationen.⁷

Zur Informations- und Datenverarbeitung werden Hardwarekomponenten, Softwarekomponenten, Netzwerke und Menschen eingesetzt, die Schutz bedürfen. Es werden Server und Clients verwendet, welche durch Netzwerke mit einander verbunden sind, hier meist lokale Netze. Aber auch der Zugriff über drahtlose Netze für Personell Digital Assistant (PDA) oder Notebooks sind gängige Praxis zum Austausch von Daten. Somit gilt es, sowohl die Server

¹ Vgl. o. V. (2008), Datendiebstahl unter www.faznet.de [15.10.08].

² Vgl. o. V. (2008), Sicherheitsleck bei der Telekom unter www.spiegelonline.de [15.10.08].

³ Vgl. Lassmann (2006), S. 349.

⁴ Vgl. Wirtz (2001), S. 16.

⁵ Vgl. Kall (2008), S. 3.

⁶ Vgl. Baier et. al. (2003), S. 179.

⁷ Vgl. Lassmann (2006), S. 349.

und Clients sowie die zugehörigen Netze zu sichern, damit keine unbefugten Personen, sei es von außen oder von innen, Daten aus den Systemen entwenden oder Viren, Würmer, Trojanische Pferde oder andere Schädlinge ins System einschleusen können.⁸

Neben der Sicherung der Hardware muss der Mensch, der tagtäglich mit der Technik arbeitet, mit in ein geeignetes Sicherheitskonzept eingebunden werden, da auch der Mitarbeiter ein Risiko darstellt.⁹ Hierbei lassen sich die jeweiligen Mitarbeiter idealtypisch in unterschiedliche Menschenbilder eingruppiert,¹⁰ so dass dem jeweils zugrunde liegenden Menschenbild entsprechend differenziert auf die Mitarbeiter eingegangen werden muss, diese somit seitens der Führungsebene unterschiedlich geführt werden müssen.

Informationssicherheit muss bereits in der Unternehmenskultur verankert sein und in eine Sicherheitskultur eingebettet sein, um dediziert auf die einzelnen Stellen und Funktionen herunter gebrochen zu werden. Essentiell für die Informationstechnologie ist es, eine IT-Sicherheitsstrategie zu entwickeln,¹¹ die die Maßnahmen im Falle eines Zwischenfalles regelt.

1.2 Vorgehensweise der Arbeit

Zunächst sollen im zweiten Kapitel die Grundlagen der Informationssicherheit, wie die rechtlichen Bedingungen, die Sicherheitsstrategie, die Sicherheitsziele und IT-Sicherheit als Service erörtert werden.

Das dritte Kapitel beschäftigt sich im Folgenden näher mit den durch den Einsatz von IT-Anwendungen entstehenden Bedrohungen, die intern oder extern das Unternehmen angreifen können. Zudem soll ferner auf die Abhängigkeit der Unternehmen von der Informationstechnologie (IT) sowie die damit verbundenen Risiken eingegangen werden.

In Kapitel vier werden dann die Komponenten der IT aufgezeigt. Dabei wird auf der einen Seite auf die Hard- und Software und auf der anderen Seite auf die Akteure, also die Entscheider, Entwickler, Administratoren und die Nutzer eingegangen. Des Weiteren werden nochmals die Akteure aufgegriffen sowie zwei Typologien aus der betriebswirtschaftlichen Literatur beschrieben, die die unterschiedlichen Menschenbilder innerhalb eines Unternehmens charakterisieren.

Ein ganzheitliches Konzept zur Einbindung sowohl der Hardware, der Software, der Netze als auch der differenzierten Menschenbilder soll in Kapitel 5 dargestellt werden, da die Akteure,

⁸ Vgl. Brechtold (2003), S. 11.

⁹ Vgl. Schlienger (2007), S. 487; vgl. Mix/Pingel (2007), S. 498, vgl. Zerr (2007), S. 519; vgl. Fox (2003), S. 676; vgl. Schimmer (2007), S.510; vgl. Baier/Straub (2005), S. 313; Fox/Kaun (2005), S. 329; vgl. Schultz (2005), S. 426.

¹⁰ Vgl. Schein (1980), S. 52.

¹¹ Vgl. von Solms/von Solms (2004), S. 372.

und hier vor allem die eigenen Mitarbeiter,¹² ein entscheidendes Sicherheitsrisiko für die IT-Infrastruktur der Unternehmen darstellen. Um diese Risiken zu minimieren, bedarf es einer Einbindung der Mitarbeiter in das Sicherheitskonzept, denn auch hierbei gilt es, das schwächste Glied einer Kette zu stärken,¹³ indem geeignete Maßnahmen zur Schließung von Sicherheitslücken ergriffen werden. Gleichzeitig gilt es aber auch, die anderen Komponenten (Hardware, Software und Netze) im Rahmen des vorgegebenen Budgets zu sichern, wobei jedoch eine Balance zwischen den einzelnen Sicherheitsmaßnahmen gefunden werden muss, damit nicht ein Bereich vernachlässigt wird, wie es bislang mit dem Personalbereich geschehen ist.

Zuletzt soll in Kapitel 6 ein Fazit und ein Ausblick zu dem in dieser Arbeit erstellten Konzept und zu der Informationssicherheit im Allgemeinen gegeben werden.

Die Vorgehensweise wird in der nachfolgenden Abbildung illustriert dargestellt:

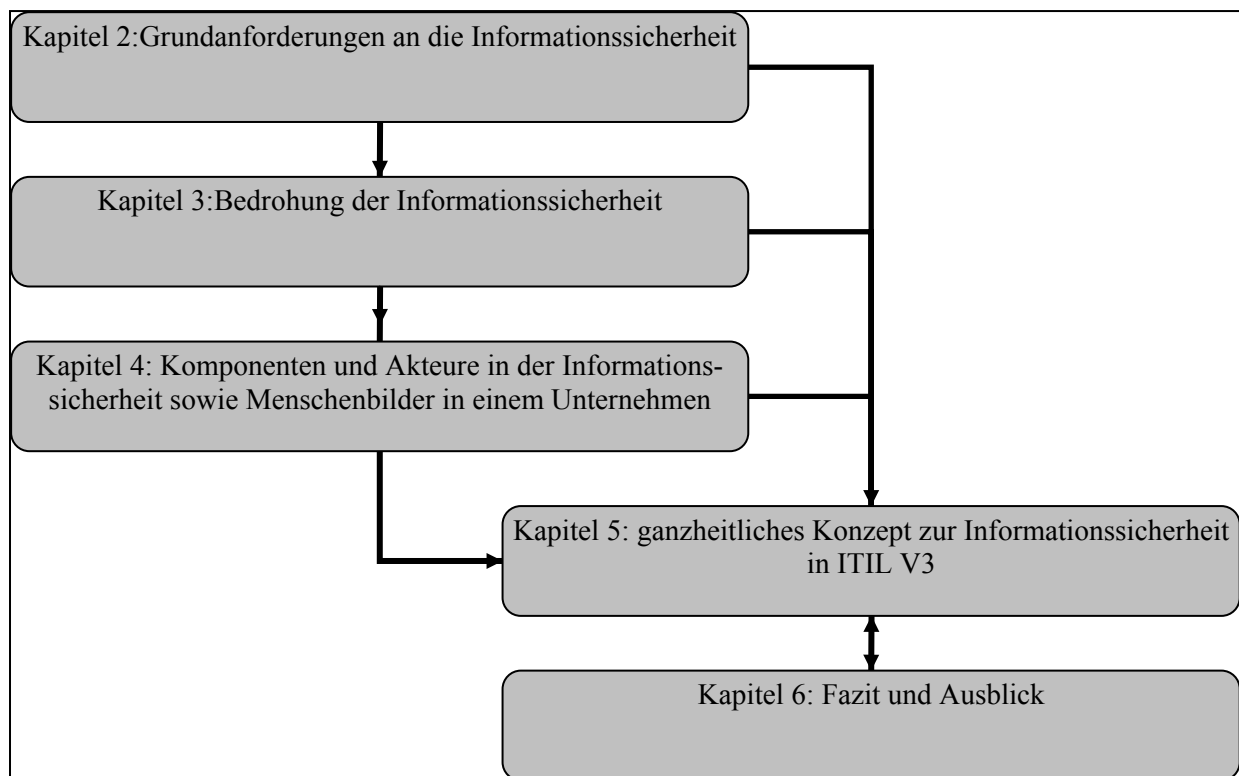


Abbildung 1: Vorgehensweise der Arbeit
Quelle: eigene Darstellung

¹² Vgl. Deloitte (2007), S. 25.

¹³ Vgl. Schimmer (2007), S. 510.

sollte zu den Abweichungen aus seiner Sicht Stellung nehmen können und die Gründe hierfür darlegen.⁴³⁸

Die Kontrolle dient weiterhin der Überprüfung der Angemessenheit und Wirksamkeit der Schutzmaßnahmen.⁴³⁹ Wird eine Abweichung festgestellt, so sind die abweichenden Maßnahmen zu verbessern oder durch andere zu ersetzen, um das angestrebte Sicherheitsniveau zu erreichen.

Obwohl die Kosten für die Informationssicherheit schwer zu ermitteln sind, ist die Durchführung einer Kostenkontrolle empfehlenswert, um das Budget einzuhalten und zu budgetlastige Maßnahmen durch günstigere auszutauschen, so dass die Wirtschaftlichkeit der Informationssicherheit gewahrt bleibt.⁴⁴⁰

6 Fazit und Ausblick

6.1 Fazit

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 Assessment Center 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 muss von den Managern erkannt werden, damit entsprechende Budgets für Schutzmaßnahmen bereitgestellt werden. Ihre Vorbildfunktion den

⁴³⁸ Vgl. Schmidt (2007), S. 527.

⁴³⁹ Vgl. Hofmann (2007a), S. 260.

⁴⁴⁰ Vgl. BSI (2008a), S. 83.

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 verursacht⁴⁴¹ und folglich eine 100%-ige Sicherheit nicht zu realisieren ist.⁴⁴²

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, d. h. den Menschen, nicht berücksichtigen oder Sicherheitslücken anderer Maßnahmen nicht schließen und somit ineffizient sein. Die Wechselwirkungen zwischen den Maßnahmen sind hierbei zu berücksichtigen, so können die besten technischen Maßnahmen verpuffen, wenn die Mitarbeiter nicht wissen, wie man mit diesen umgeht oder welche weiteren Maßnahmen eingeleitet werden müssen, nachdem die technischen Maßnahmen erfolgreich gegriffen haben. Nur wenn obige Bedingungen erfüllt sind, kann das Business Continuity durch das richtige Verhalten der Mitarbeiter gewährleistet werden, um finanzielle Schäden aber auch Reputationsschäden zu vermeiden.

Das vorliegende Sicherheitskonzept geht verstärkt auf die personellen Maßnahmen ein, da sie in den Unternehmen zum Teil 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, da z. B. das IT-Grundschutzhandbuch mehrere hundert Schutzmaßnahmen anspricht, die realisiert werden können. Zudem muss sich das Konzept noch in der Praxis beweisen.

Das Outsourcing der Informationssicherheit ist nur dann empfehlenswert, wenn keine geschäftskritischen Prozesse bzw. deren unterstützende IT ausgelagert werden, es sei denn es wird im eigenen Unternehmen in Form eines SSC ausgegliedert, wo die Schutzziele weiterhin gewahrt bleiben und eine Abhängigkeit von einem Dritten nicht besteht. So wiederum lassen sich durch Skaleneffekte Kostenreduzierungen erzielen und die Prozesse sicherer und effizienter gestalten.

⁴⁴¹ Vgl. Pohlmann (2006), S. 28f.

⁴⁴² Vgl. Humpert (2004), S. 16.

ITIL als good practice De-facto-Standard vermittelt ein gutes Rüstzeug für die Informationssicherheit, wie z. B. die prozessualen Maßnahmen, jedoch werden die personellen Maßnahmen nur teilweise berücksichtigt, so dass hier Nachholbedarf besteht. Daher wurde das Information-Security Management in ITIL V3 durch dieses ganzheitliche Sicherheitskonzept zum Teil bezüglich der personellen und technischen wie aber auch der physikalischen Maßnahmen erweitert und ergänzt, so dass ein größerer Schutz vor dem Risikofaktor Mensch gegeben ist.

6.2 Ausblick

Die Bedrohungen der Informationssicherheit werden auch in Zukunft existent sein, wobei sich jedoch die Art ändern kann. Die Brisanz des Themas wird sich eher noch zuspitzen, denn wie erwähnt, sind die Unternehmen zum Großteil von der IT abhängig. Neue Techniken und Verfahren werden, wie in der Vergangenheit, auch zukünftig für Bedrohungen sorgen, die wiederum durch neue technische, prozessuale, physikalische aber auch personelle Maßnahmen bekämpft werden. Dabei müssen immer erst die Bedrohungen auftreten und meist auch Schäden anrichten, damit Schutzmaßnahmen entwickelt und angewendet werden können.

Es wird demzufolge für die Informationssicherheit weiterer Forschungsbedarf bestehen, 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 sind Unternehmen in der Lage, Mitarbeiter einzustellen, die sich sicherheitskonform verhalten werden und zum Schutz der Informationssicherheit, ihrer Systeme, Daten und Informationen beitragen. Zur Einstellungsermittlung müssen Unternehmen diese Verfahren einführen. Die Weiterbildungen im Rahmen der Informationssicherheit sollten in regelmäßigen Abständen erfolgen, wobei die Mitarbeiter gleichzeitig Spaß an der Teilnahme haben sollte aber auch das Gelernte in die Tat umsetzen können sollten. Wie solche Schulungen oder Fortbildungen am effizientesten zu gestalten sind, ist noch zu entwickeln.

Die Informationssicherheit, obwohl als notwendig erachtet, darf 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, wobei sie die Informationssicherheit nicht beachten und Schäden anrichten, entgegen zu wirken.⁴⁴³

⁴⁴³ Vgl. Pokoyski (2006), S. 1f.