universität wien

MASTERARBEIT

Titel der Masterarbeit

„Schaffung eines nachhaltigen IT-Security Managementkonzepts für kleine und mittlere Unternehmen“

Verfasser

Manuel Siebenhandl, Bakk.rer.soc.oec

angestrebter akademischer Grad

„Diplom-Ingenieur“ (Dipl.-Ing. bzw. DI)

Wien, 2011

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Masterstudium Wirtschaftsinformatik UG2002
Betreuerin / Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

DANKSAGUNG

Mein Dank richtet sich an Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr, der es mir ermöglicht hat, eine meinen Interessen entsprechende Masterarbeit zu verfassen und auch während der Entstehung für konstruktive und freundliche Betreuung stets zur Verfügung stand.

Ebenso möchte ich mich bei der ViaDonau – Österreichische Wasserstraßen-Gesellschaft mbH bedanken, insbesondere bei Herrn Dipl. Ing. Hans-Peter-Wegscheider und Herrn Slobodan Vucinic, die es mir gestatteten, einen für mich wertvollen Praxisbezug in dieser Arbeit herzustellen.

Besonderer Dank gilt auch meiner Familie und Freunden, die mir stets mental beistanden und somit den Werdegang meiner Arbeit positiv beeinflusst haben. Hervorheben möchte ich jedoch meine Eltern Reinhard und Margit Siebenhandl, die es mir überhaupt ermöglicht haben, das Studium abzuschließen und mich in den letzten Jahren stets mit Rat und Tat, aber auch mit viel Geduld auf meinem Werdegang begleiteten.

Inhaltsverzeichnis

1 Problembeschreibung

In den letzten Jahren entwickelte sich das Thema IT-Security zu einer immer essentielleren Disziplin in Unternehmen weltweit. Ursprünglich als eine Sparte angesehen, die als nettes Add-On dient, rückt IT-Security bei der Planung und Einrichtung von IT-Infrastrukturen von Konzernen in das Zentrum. Diverse Umfragen in Medien zeigen, dass das Thema Sicherheit zu einer der Hauptprioritäten im Informations- und Kommunikationstechnologiebereich wird. Spezielle Begriffe wie „Security Management“ und „Information Security“ rücken in den Mittelpunkt von IT-Experten in den heutigen Unternehmen. Eine wesentliche Aufgabe besteht darin, adäquate IT-Architekturen, koordinierte Technologieführung und Definition von Rollen und Verantwortungsbereichen über das ganze Unternehmen hinweg zu schaffen. Dies alles sollte unter Berücksichtigung von etablierten Security Richtlinien, Standards und Methoden ermöglicht werden. Stärken und Schwächen bestehender Systeme müssen analysiert werden, um notwendige Korrekturen durchzuführen und eine kontinuierliche Verbesserung sowohl der IT-Landschaft, als auch des Sicherheitsbewusstseins innerhalb der Unternehmen zu gewährleisten.

Seitdem der Einfluss von elektronisch Aktivitäten wie E-Business, E-Leisure, E-Payment, und E-Social Computing enorm zugenommen hat und zu einem immer größeren Teil über das Internet abgewickelt wurde, stieg auch die Anforderung an das Themengebiet der Security, einen gewissen Standard an Datenschutz, Vertrauen, Verlässlichkeit, Sicherheit und Nachvollziehbarkeit zu gewährleisten. Eine Vielzahl von Kerngeschäftsprozessen heutiger Unternehmen wird elektronisch gesteuert, große Mengen von Informationen sind digital gespeichert und werden in Netzen übermittelt. Nahezu niemand mehr kann auf die Verwendung des Internets verzichten, seien es Finanzinstitutionen, staatliche als auch nichtstaatliche Einrichtungen, Commercial Traders, Service Providers oder einfach nur Privatpersonen. Dies allein spiegelt den immensen Einfluss von Security als Schlüsseltechnologie im

heutigen Unternehmensumfeld wider, speziell in Anbetracht dessen, dass das Internet für ein Fehlen an Sicherheit bekannt ist, aber auch, dass viele kommerzielle Applikationen Lücken aufweisen und dadurch ein großes Gefahrenpotential darstellen. Die Fehleranfälligkeit von Applikationen, der Mangel an Sicherheitsvorkehrungen innerhalb von Unternehmen, die über das Internet agieren, sowie Angriffe auf deren Systeme können zu enormen Verlusten/Schäden sowohl finanzieller Natur, als auch in Hinsicht auf das Image bis hin zur Gefährdung des Kerngeschäfts führen.

Um die Zunahme der Bedeutung von IT-Security in Unternehmen darzustellen, sowie diese anhand von Kennzahlen zu präsentieren, wird jährlich der „CSI Computer Crime & Security Survey“ [Rich08] veröffentlicht. Es handelt sich hierbei um eine Umfrage basierend auf der Befragung von Security Fachleuten, die in diversen Sektoren wie Finanz, Consulting, Information Technology, Gesundheit usw. tätig sind. Resultate und deren anschließende Analysen stützen sich auf den Survey aus dem Jahr 2008, welcher von 518 Befragten beantwortet wurde.

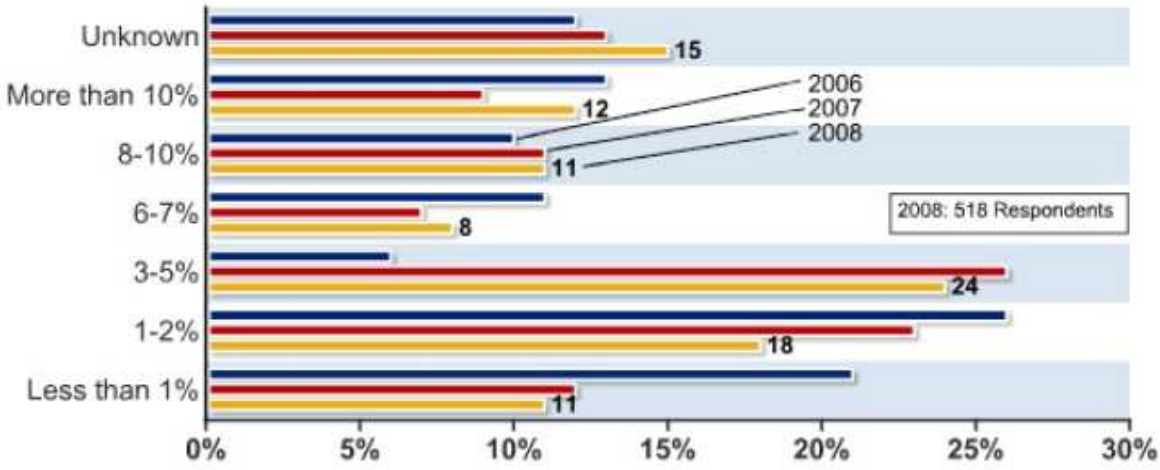


Abbildung 1: Prozentsatz des IT-Budgets für Security [Rich08]

Wie bereits anfangs erwähnt wird die IT-Security nicht nur mehr als nettes Add-On in den Unternehmen gesehen, sondern stellt zu einem immer größer werdenden Teil einen zentralen Baustein in der Budgetierung dar.

In Abbildung 1: Prozentsatz des IT-Budgets für Security spiegelt sich die Entwicklung in Prozentpunkten des IT-Budgets, welches in den Bereich der Security investiert wird, wider. Hierbei werden die Abweichungen der Resultate der Surveys der Jahre 2006 - 2008 verglichen. Grundsätzlich lässt sich ein steigendes Sicherheitsbewusstsein erkennen, da verglichen zum Jahr 2006 ein prozentueller Anstieg bei der Budgetierung des IT-Security Budgets erkennbar ist. Im Jahr 2006 wurden von einem Großteil lediglich 1 bis 2% oder weniger in den Bereich IT-Security investiert. Betrachtet man die Abbildung in Hinblick auf das Jahr 2008 wird ersichtlich, dass eine Mehrzahl der Unternehmen zumindest 3-5% in den Bereich Security investiert hat. Andererseits sieht man auch, dass es tendenziell zu einer leichten Reduzierung der Investitionen im höheren Prozentbereich gemessen an den Vorjahren kam. Grundsätzlich kann aber der Schluss gezogen werden, dass das Bewusstsein bezüglich Security zunimmt, wenn man betrachtet, dass im Jahr 2008 53% der Befragten angaben, 5% oder weniger in den Security Bereich zu investieren, verglichen zum Jahr 2007, in dem es noch 61% waren [Rich08].

Ein weiterer nicht außer Acht zu lassender Punkt hinsichtlich der Bedeutung von Security in Unternehmen ist die Anzahl der durchgeführten Awareness-Trainings. Mittels dieser Trainings hat man sich zum Ziel gesetzt, Mitarbeiter bzw. Angestellte im Umgang mit sensiblen Unternehmensdaten korrekt und verantwortungsvoll zu schulen. In Abbildung 2 sieht man anhand einer Gegenüberstellung der Jahre 2007 und 2008 die prozentuale Entwicklung des Budgeteinsatzes in Awareness-Trainings.

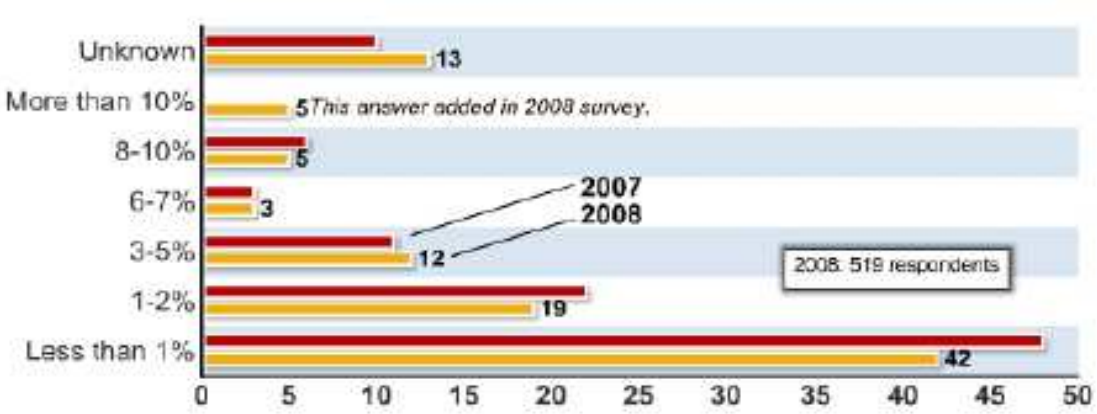


Abbildung 2: Prozentsatz des IT-Budgets für Awareness-Trainings [Rich08]

Aus der Grafik wird ersichtlich, dass auch heute noch ein Großteil der Unternehmen nur einen geringen Anteil des IT-Budgets in Awareness-Trainings investiert. Die Autoren des CSI Computer Crime & Security Survey führen diesen geringen Prozentsatz darauf zurück, dass immer noch eine mangelnde Akzeptanz hinsichtlich des Mehrnutzens dieser Art von Trainings, sowohl für die Mitarbeiter als auch für die Unternehmen besteht. Eine weitverbreitete Annahme ist, dass Angestellten durch die Trainings Arbeitszeit verloren geht, während der sie produktiv tätig sein könnten. Setzt man sich aber näher mit der Thematik Security in Unternehmen auseinander, kann festgestellt werden, dass der Faktor Mensch von ziemlicher Bedeutung für genau diesen Bereich ist. Oftmals gelangen sensible Unternehmensdaten durch das Fehlverhalten von Mitarbeitern in falsche Hände, sei es durch den falschen Umgang mit vorhandener Software, der willkürlichen Weitergabe von unternehmensinternen Daten, oder weil man sich den Gefahren im Internet einfach nicht bewusst ist [Rich08]. Diese Problematik wäre mittels Mitarbeiter Awareness-Trainings einfach zu lösen.

1.1 Zielsetzung der Arbeit

Die Zielsetzung dieser Masterarbeit ist die Schaffung eines nachhaltigen IT-Security Managementkonzepts für kleine und mittlere Unternehmen (KMU). Dies erfolgt unter Berücksichtigung der im deutschsprachigen Raum meistverbreiteten existierenden Planungsansätze der IT-Security. Zu diesen zählen die ISO-2700x Normreihe, der IT-Grundschutzkatalog bzw. die IT-Grundschutzvorgehensweise des Bundesamts für Sicherheit in der Informationstechnik (BSI), in Österreich das österreichische Informationssicherheitshandbuch, sowie der Common Criteria for Information Technology Security Evaluation Standard (CC) zur Bewertung der Sicherheit von Informationstechnologie.

Aufbauend auf die existierenden Planungsansätze, sowie die in der Arbeit identifizierten bestehenden und zukünftigen Herausforderungen für den Entwurf eines IT-Security Managementkonzepts für KMUs werden Anforderungen abgeleitet. Diese werden in weiterer Folge in ein Konzept eingearbeitet, welches sicherstellen soll, dass mit vertretbarem Aufwand ein umfassender und nachhaltiger Beitrag zur Verbesserung der IT-Security in KMUs gewährleistet werden kann. Der nachhaltige Beitrag wird unter anderem dadurch garantiert, dass neben der Berücksichtigung existierender Planungsansätze und Best Practices, Trends hinsichtlich der IT-Security, die in den nächsten 3-4 Jahren immer mehr an Bedeutung gewinnen werden, ebenfalls berücksichtigt sind. Es wird kleinen und mittleren Unternehmen ein einfaches Vorgehenskonzept zur Verfügung gestellt, welches ihnen ermöglicht, schnell effiziente Maßnahmen zur Einrichtung eines nachhaltigen IT-Security Managements auszuwählen und durchzuführen. Die Überprüfung auf Praxistauglichkeit des entwickelten Konzepts erfolgt anschließend in Kooperation mit der Via Donau - Österreichische Wasserstraßen-Gesellschaft mbH.

1.2 Gliederung der Arbeit

Die Arbeit ist in fünf Abschnitte unterteilt. Der erste Teil, welcher die Kapiteln 2 und 3 umfasst, beinhaltet Definitionen und theoretische Grundlagen zum Thema IT-Security.

Der zweite Teil besteht aus Kapitel 4, in welchem existierende Planungsansätze bezüglich der IT-Security untersucht und erläutert werden. Diese dienen als eine der Grundlagen, beziehungsweise notwendiger Input zur Erstellung eines nachhaltigen IT-Security Managementkonzepts. Darüber hinaus wird ein kurzer Überblick über derzeitige wissenschaftliche Forschungsaktivitäten in diesem Themengebiet gegeben.

Der dritte Teil der Arbeit setzt sich aus den Kapiteln 5 und 6 zusammen und bildet mit dem vierten Teil den Schwerpunkt dieser Arbeit. Hierbei werden die wesentlichen Herausforderungen und daraus abgeleitet die Anforderungen für die anschließende IT-Security Managementkonzepterstellung erhoben.

Der vierte Teil besteht aus den Kapiteln 7 und 8 und beinhaltet den konkreten Entwurf des nachhaltigen IT-Security Managementkonzepts für KMUs, basierend auf den identifizierten Herausforderungen und Anforderungen des vorherigen Abschnitts. Zusätzlich fließt vorhandenes Wissen aus den existierenden Planungsansätzen in die Entwicklung ein. In Kapitel 8 wird anhand einer Case Study das entworfene Konzept auf seine Praxistauglichkeit anhand eines realen Unternehmens überprüft und angewandt. Die Erstellung der Case Study erfolgt in Zusammenarbeit mit der „via donau – Österreichische Wasserstraßen-Gesellschaft mbH“.

Im fünften und letzten Teil der Arbeit wird auf die Ergebnisse der Arbeit Bezug genommen, sowie eine persönliche Reflektion der gewonnen Erkenntnisse vorgenommen. Des Weiteren wird auf die Grenzen hinsichtlich Abdeckung und Umsetzung des Konzepts eingegangen und ein Ausblick für die Zukunft gegeben.

2 Grundlegende Definitionen

Der Oberbegriff der „Information Security“ beinhaltet das Information Security Management, Netzwerksicherheit, Computer- und Datensicherheit sowie Policies. Um das Themengebiet der Information Security zu verstehen, gilt es zu erkennen, inwiefern die einzelnen Teilbereiche einzuordnen sind, sich überschneiden, oder aber auch abgrenzen (siehe Abbildung 3).

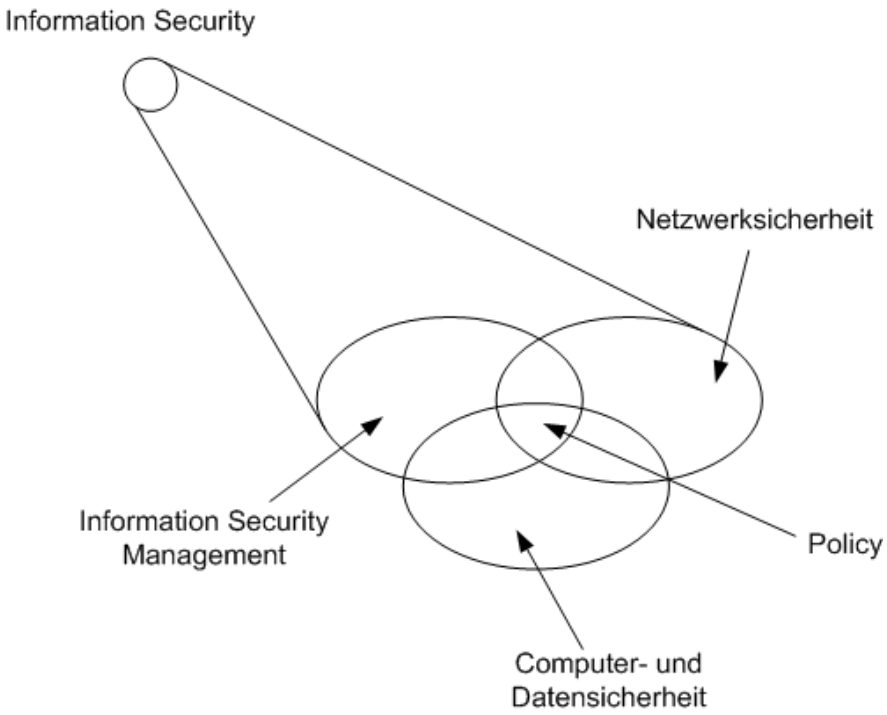


Abbildung 3: Komponenten der Information Security nach [Qui09]

Information Security Management ist ein Teil des Themengebiets der Information Security. Durch ein angemessenes Security Management wird die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gewährleistet. Weitere Eigenschaften wie Authentizität,

Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit werden ebenfalls diesem Gebiet zugeordnet [ISO10].

Weiters gilt es zu definieren, was unter den Paradigmen der **Nachhaltigkeit** (Sustainability), **Wartbarkeit** (Maintainability) und **Skalierbarkeit** (Scailability) zu verstehen ist, auf denen das in dieser Arbeit entworfene IT-Security Managementkonzept beruht. Darüber hinaus werden in einem weiteren Unterkapitel die wesentlichen **Schutzziele** der IT-Security und deren Bedeutung erläutert. Die Schutzziele bilden das Fundament für ein funktionierendes Sicherheitskonzept.

2.1 Nachhaltigkeit/ Sustainability

Der Begriff der Nachhaltigkeit hat seinen Ursprung im 18. Jahrhundert und wurde im Rahmen der fortschreitenden Abholzung der Wälder in der Forstwirtschaft formuliert. Durch die immense Rodung der Wälder und deren langer Regenerationsdauer sowie geringen Wachstumsraten erlangte das Konzept der nachhaltigen Bewirtschaftung in diesem Zusammenhang große Bedeutung in Hinblick auf den schonenden und effizienten Umgang mit Ressourcen [Wei03].

Nach Jens Pientak [Pie10] definiert sich die Nachhaltigkeit in der IT durch eine ökologische, ökonomische und soziale Dimension. Die ökologische IT, auch als „Green IT“ bezeichnet, bezieht sich auf die ökologische Komponente; zum Beispiel die Steigerung der Energieeffizienz von Hardware. Die ökonomische Dimension umfasst Einsparungspotentiale in der IT, zum Beispiel über geringere Betriebskosten. Die soziale Komponente beschäftigt sich mit der Integration der Nachhaltigkeit in der Unternehmensphilosophie [Pie10].

Im Rahmen dieser Arbeit versteht man unter dem Begriff der Nachhaltigkeit die Schaffung eines IT-Security Managementkonzepts, welches den ständig ändernden Sicherheitsherausforderungen bzw. Anforderungen gerecht wird und diese berücksichtigt. Seien es Änderungen im organisatorischen und technologischen Bereich des Unternehmens oder Herausforderungen in Form

von neuen Bedrohungsszenarien. Durch die Nachhaltigkeit wird gewährleistet, dass das entwickelte IT-Security Managementkonzept dergestalt konzipiert ist, dass sowohl auf beabsichtigte Veränderungen als auch auf künftig zufällig auftretende entsprechend reagiert werden kann.

2.2 Wartbarkeit/ Maintainability

Der Begriff der Wartbarkeit wird oftmals in Zusammenhang mit der Softwareentwicklung verwendet und bezieht sich auf den Aufwand für Änderungen im Softwareentwicklungsprozess. In der ISO-Norm 9126 wird die Wartbarkeit als ein Qualitätsmerkmal definiert, welches ein Softwareprodukt befähigt, modifiziert zu werden. Hierzu gehören beispielsweise Korrekturen, Verbesserungen und Anpassungen der Software an Änderungen der Umgebung [RB09].

Im Rahmen dieser Arbeit ist unter der Wartbarkeit zu verstehen, dass das entworfene IT-Security Managementkonzept die Qualität besitzen muss, auf entsprechende Herausforderungen und Anforderungen, wie bereits im Kapitel 2.1 erwähnt, einzugehen und entsprechend zu reagieren. Nur so kann auch das zuvor beschriebene Konzept der Nachhaltigkeit erfüllt werden. Betrachtet man die sich ständig ändernden Herausforderungen im Bereich der IT-Security, erkennt man, dass das Thema der Wartbarkeit unerlässlich für Unternehmen ist, um längerfristig für die Herausforderungen im Alltag gewappnet zu sein.

2.3 Skalierbarkeit/ Scailability

Die Skalierbarkeit bietet nach [KP10] Computern oder Software die Fähigkeit, sich wachsenden Ansprüchen anzupassen. Das in dieser Arbeit entworfene IT-Security Managementkonzept muss dem Paradigma der Skalierbarkeit entsprechen. Ändern sich beispielsweise die Leistungsanforderungen an das Unternehmen, das Geschäftsmodell oder ein Unternehmensziel, muss gegebenenfalls die Möglichkeit bestehen, die IT-Security im Hintergrund effektiv auf die neuen Anforderungen auszurichten.

2.4 Schutzziele

Grundsätzlich lässt sich sagen, dass IT-Security auf folgenden wesentlichen Prinzipen beruht: **Vertraulichkeit, Integrität**, **Verfügbarkeit** und **Verbindlichkeit**. Je nach Kontext in dem diese grundlegenden Aspekte auftreten, können sie unterschiedlich interpretiert werden, abhängig vom Umfeld, Bedürfnis und den Gesetzen innerhalb eines bestimmten Unternehmens.

2.4.1 Vertraulichkeit/ Confidentiality

Die Vertraulichkeit bezieht sich auf den Schutz bzw. die Geheimhaltung von Informationen und Ressourcen. Der Ursprung liegt in der Notwendigkeit, in sensiblen Bereichen wie Industrie und Regierungen Informationen zu schützen.

Der Zugang zu Informationen und Daten soll nur jenen Benutzern ermöglicht werden, die dafür auch autorisiert sind, diese zu sehen oder zu modifizieren. Zugangskontrollmechanismen sind ein grundlegender Baustein, um Vertraulichkeit zu gewährleisten. Ein Beispiel hierfür wäre die moderne Kryptographie. [Bis03]

2.4.2 Integrität/ Integrity

Die Integrität bezieht sich auf die Vertrauenswürdigkeit von Daten und Ressourcen und zielt auf den Schutz vor unzulässiger und unautorisierter Veränderung von Daten ab. Integrität beinhaltet zum einen die Datenintegrität (der Inhalt der Daten), zum anderen die Integrität der Datenquelle, welche auch oftmals als Authentizität (Echtheit) bezeichnet wird und gewährleistet sein muss. Weiters unterscheidet man zwischen zwei Klassen von Integritätsmechanismen, zum einen dem Schutzmechanismus, zum anderen dem Nachweismechanismus [Bis03].

Der Schutzmechanismus hat zum Ziel, die Datenintegrität aufrecht zu erhalten, indem versucht wird, unrechtmäßige Datenveränderungen jeglicher Form zu verhindern. Es soll dadurch verhindert werden, dass Daten in unerlaubter Form verändert werden, beziehungsweise von Personen, die dazu nicht berechtigt

sind. Der Nachweismechanismus hat nicht zum Ziel, Verletzungen bezüglich der Integrität sicherzustellen, sondern nachzuweisen, dass die Integrität bestimmter Daten nicht mehr vertrauenswürdig ist. Diese sogenannten Nachweismechanismen dienen zur Analyse möglich auftretender Ereignisse innerhalb eines Systems (z.B. Aktionen durchgeführt durch einen User) und der Datenanalyse, um festzustellen, ob eventuelle Veränderungen an Daten vorgenommen wurden. [Bis03]

Vertraulichkeit und Integrität stehen in engem Zusammenhang; mittels Vertraulichkeit wird versucht zu garantieren, dass Daten nur jenem Personenkreis zugänglich gemacht werden, für den die Informationen auch relevant sind. Integrität beinhaltet darüber hinaus noch die Korrektheit und die Glaubwürdigkeit der Daten. Dies beginnt schon bei der Quelle, von wem und woher kommen die Daten, wie gut waren sie bei der Übertragung geschützt, bevor sie an ihrem Ziel eingetroffen sind und kann darüber hinaus auch ein ausreichender Schutz in Zukunft gewährleistet werden.

2.4.3 Verfügbarkeit/ Availability

Die Verfügbarkeit spiegelt die Fähigkeit wider, Informationen und Ressourcen jederzeit zu nutzen, wann auch immer sie benötigt werden [Bis03]. Die Verfügbarkeit ist ein wichtiger Aspekt hinsichtlich der Verlässlichkeit eines Systems, da ein nicht erreichbares System mindestens genauso schlecht ist, wie das Nichtvorhandensein eines Systems. Bezüglich Security ist die Verfügbarkeit deshalb wichtig, da dadurch verhindert werden soll, dass der Zugriff auf Daten oder Services eines Systems durch Manipulation vorsätzlich unerreichbar gemacht wird. Ein gängiges Beispiel, um die Verfügbarkeit eines Systems zu beeinträchtigen, sind „Denial of Service Attacks“.

Zusammenfassend könnte man sagen, dass der Begriff Security in Bezug auf die drei zuvor vorgestellten grundlegenden Komponenten folgendes Ziel hat: *„Aufrechterhaltung beziehungsweise Umsetzung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit unter Berücksichtigung der*

menschlichen Komponente, um maximale Protektion innerhalb von IT-Landschaften zu gewährleisten“.

2.4.4 Verbindlichkeit/ Non-Repudiability

Die Verbindlichkeit steht dafür, dass Veränderungen an Informationen und Ressourcen nachträglich eindeutig einer Person zuordenbar sein müssen. Es soll dadurch gegenüber einem Dritten jederzeit nachgewiesen werden können, wer zuletzt auf Informationen und Ressourcen zugegriffen hat. Die Eigenschaft der Verbindlichkeit schließt die Eigenschaften der Authentizität und der Integrität mit ein. Die Gewährleistung der Verbindlichkeit erfolgt in der Praxis meistens durch eine händische bzw. digitale Unterschrift oder durch eine digitale Signatur [SSP08].

3 Risiko, Gefahr und Missbrauch

Wie bereits in der Problembeschreibung erwähnt, gibt es eine Vielzahl an Gefahren und Risiken für Unternehmen betreffend ihrer IT-Infrastrukturen. Im folgenden Kapitel werden die Risikofaktoren, die bestehenden Gefahren und die Arten des Missbrauchs von IT-Systemen erläutert und klassifiziert. Darüber hinaus werden die Angriffspunkte bzw. Verwundbarkeiten eines Unternehmens beschrieben, sowie die Auswirkungen und Konsequenzen eines Sicherheitsbruchs, die ein auf IT gestütztes Unternehmen erleiden kann. Durch die aufgezeigten Risiken, Gefahren und verschiedenen Typen von Missbrauch der IT-Systeme lassen sich wie nachfolgend angeführt, die Ziele der IT-Security ableiten.

3.1 Risikofaktoren in der IT

Durch die zunehmende Globalisierung und Vernetzung der Konzerne, sowie die Verlagerung und Abwicklung vieler Kerngeschäftsaktivitäten über das Internet entstanden im letzten Jahrzehnt zunehmend neue Risiken und Bedrohungen, die es zu bewältigen gilt. Bevor man sich aber intensiver mit diesem Themenbereich auseinandersetzt, müssen grundlegende Schlüsselwörter erläutert werden, um die Zusammenhänge bzw. Faktoren zu verstehen, die für IT-Security relevant sind.

- **Gefahren (Threats):** Hierbei handelt es sich um einen Sachverhalt, welcher zu potentiellem Schaden bzw. Verlust führen kann. Gefahren können wiederum nach [FKLP08] klassifiziert werden in:
  - Zufällig auftretende: z.B. Feuer, Stromausfall, Bedienungsfehler, usw.
  - Umweltbedingt: Überschwemmung, Blitzeinschlag, usw.
  - Beabsichtigte: z.B. Schadsoftware, Lauschangriffe, Hacking, usw.
- **Verwundbarkeit (Vulnerability):** definiert die Wahrscheinlichkeit, mit der eine Gefahr in der Realität eintritt und bezieht sich grundsätzlich auf

die Schwäche eines Systems, welches angegriffen werden kann. Die Definition von Gefahren ist allgemein und von generischer Struktur. Hingegen handelt es sich bei der Verwundbarkeit um eine spezifische Definition in Bezug auf ein bestimmtes System und Maßnahmen, um dieses zu schützen [FKLP08].

- **Asset (Werte):** umfasst alle wichtigen Teile eines Unternehmens, beispielsweise Hardware, Software, Wissen und Individuen. [FKLP08]

- **Risiko (Risk):** ergibt sich aus den Gefahren und Verwundbarkeiten bezüglich eines bestimmten oder mehrerer Assets. Ziel ist es, die Verwundbarkeit der Assets eines Systems bezüglich relevanter Gefahren möglichst klein zu halten, um das Risiko zu minimieren. Dies wird meistens durch Kontrollmechanismen bewerkstelligt, welche spezifische Prozeduren oder Gegenmaßnahmen sein können. [FKLP08]

- **Wirkung (Impact):** resultiert aus einem Sicherheitsbruch, wenn ein bestimmtes Risiko eingetreten ist. Hierbei handelt es sich um ein Ereignis, welches sich aufgrund fehlender Sicherheitsvorkehrungen ergibt und spiegelt einen Mangel der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit wider. Gemessen können die Auswirkungen eines Sicherheitsbruchs in Form einer Offenlegung, Verweigerung, Zerstörung oder Veränderung von Systemen beziehungsweise deren Daten werden. [FKLP08]

- **Konsequenz (Consequence):** entspricht dem Ergebnis, welches aus einem zuvor eingetretenen Impact resultiert. Die Konsequenz resultiert aus dem Schaden, den ein Zwischenfall an einem System hervorgerufen hat. Beispiele hierfür können sein, Beeinträchtigung bzw. Unterbrechung eines Geschäftsbereichs, Gefahr für die Sicherheit der Mitarbeiter, unbeabsichtigte Offenlegung von geheimer Unternehmensinformation, Verletzung des Datenschutzes, finanzieller Verlust bis hin zur

Reduzierung des Rufs und des Firmenwerts eines Unternehmens. [FKLP08]

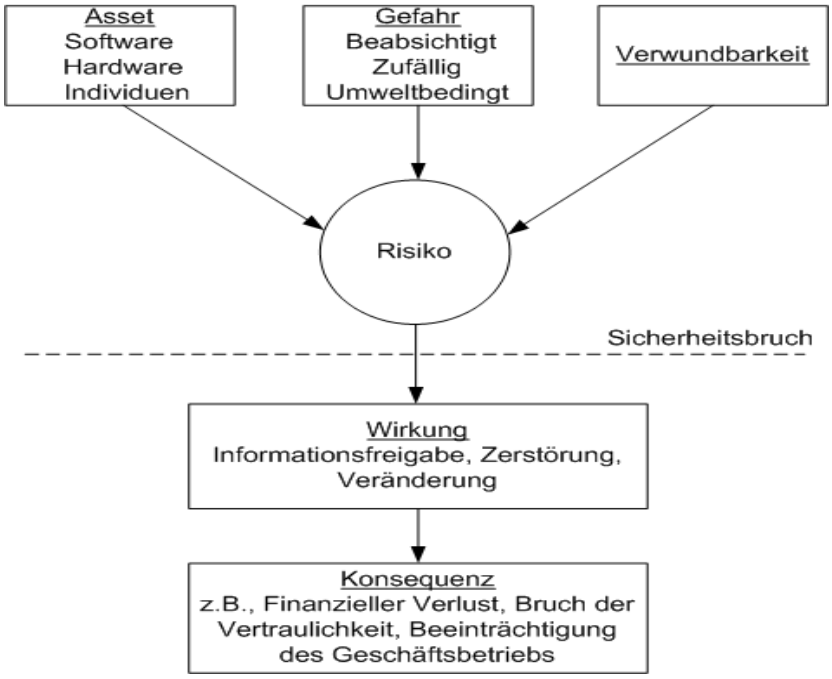


Abbildung 4: : IT-Risikofaktoren nach [FKLP08]

In Abbildung 4 sieht man, wie die bereits erwähnten Faktoren zusammenspielen und ab welchem Zeitpunkt ein Risiko Realität wird, gekennzeichnet durch den Sicherheitsbruch, sowie die daraus resultierenden Konsequenzen.

3.2 Gefahren und Verwundbarkeiten

Die zuvor bereits erwähnten Begriffe geben einen groben Überblick über die Risikofaktoren in der IT. Nun gilt es, sich diese Begriffe detaillierter anzusehen, um ein näheres Verständnis für die Zusammenhänge zu bekommen.

Um den Rahmen möglicher Gefahrenquellen vollständig abdecken zu können, werden Gefahren wie folgt gruppiert:

- **Physische Gefahrenquellen:** hierzu zählt beispielsweise Feuer, Flut, Gebäude oder Elektrizitätsversagen, usw.
- **Gefahrenquellen bezüglich der technischen Ausstattung:** CPU, Netzwerk, Speicherfehler, usw.
- **Menschliche Gefahrenquellen:** Design- oder Ausführungsfehler, falsche Anwendung von Ressourcen, verschiedene Arten von mutwilliger Zerstörung an Hardware als auch Software usw.
- **Höhere Gewalt:** Blitzschlag, Überschwemmungen, Erdbeben usw.

Ob eine Gefahr für ein Unternehmen nun ein Problem darstellt, ist abhängig von der Verwundbarkeit einer bestimmten Organisation oder eines Systems. Verwundbarkeiten bezüglich der IT-Security können in vielen Formen innerhalb eines Unternehmens auftreten. Bei der Klassifizierung gilt es zu beachten, dass nicht nur Computersysteme selbst geschützt werden sollten, sondern eine Vielzahl von anderen Faktoren, die Einfluss auf einen grundlegenden Schutz der IT-Landschaft haben. In der Literatur nach [FKLP08] werden die Verwundbarkeiten wie folgt näher spezifiziert:

1. Betriebsumfeld- und Infrastruktur Verwundbarkeiten

Zu dieser Art zählt das Fehlen von physischen Sicherheitsvorrichtungen wie zum Schutz der Gebäude, Türen und Fenster um das Eindringen von externen Personen zu verhindern und das Eigentum vor Diebstahl zu schützen. Ein weiterer Punkt, welcher in diese Kategorie fällt sind beispielsweise die Zugangskontrollen, welche zum Ziel haben sollten, dass nur jene Personen Zutritt zu Räumlichkeiten haben, die diesen auch benötigen.

2. Hardware Verwundbarkeiten

Die Hardwarekomponenten sind ein weiterer Faktor, welchen es gilt so gut wie möglich zu schützen. Zu den Verwundbarkeiten bezüglich der Hardware zählt unter anderem beispielsweise die Anfälligkeit auf Temperaturschwankungen

(Klimatisierung von Serverräumen muss gewährleistet sein) oder die Instandhaltung und Pflege von Speichermedien (kann zum Verlust von Daten bzw. zur Fehlfunktion der Medien führen).

3. Software Verwundbarkeiten

Unter diese Kategorie von Verwundbarkeiten fallen beispielsweise komplizierte User-Interfaces (können Fehlhandhabung als Konsequenz mit sich bringen), das Fehlen von Authentifizierungsmöglichkeiten und das Fehlen von Audit Trails (dadurch könnte es z.B. zu einer unautorisierten Verwendung von Software kommen) etc.

4. Kommunikationsverwundbarkeiten

Diese treten dann auf, wenn es innerhalb eines Unternehmens ungesicherte Kommunikationskanäle gibt (dies wiederum ermöglicht außen stehenden ein Abhören der übertragenen Information). Darüber hinaus ist ein großer Verwundbarkeitsfaktor das Fehlen an geschützten Netzwerkverbindungen (unautorisierte User können dadurch Zugriff auf das Firmennetzwerk erlangen und somit auch auf dessen Daten).

5. Mitarbeiter Verwundbarkeiten

Wie bereits erwähnt, stellen die Mitarbeiter einen wesentlichen Unsicherheitsfaktor dar. Um diesem Problem entgegen zu wirken, sollten Security-Trainings mit den Mitarbeitern durchgeführt werden, um ihnen die korrekte Handhabung der IT beizubringen bzw. ihr Bewusstsein im Umgang mit der IT zu stärken. Ein weiterer Faktor, um dies zu gewährleisten, ist die Einführung von regelmäßigen Monitorings, um nach zu vollziehen, wer welche Änderungen am System vornimmt und ob diese auch autorisiert sind.

3.3 Angriffe und Missbrauch auf IT-Systeme

Wie bereits angemerkt, gibt es eine Vielzahl von Gefahren und Verwundbarkeiten, die die IT-Infrastruktur eines Unternehmens gefährden können. Zurückzuführen ist dies, wie zuvor erwähnt, auf die zunehmende

Abhängigkeit der Unternehmen an elektronischer Datenverarbeitung im täglichen Geschäftsablauf über Netzwerke wie das Internet. Im folgenden Kapitel wird nun näher auf die möglichen Angriffe, sowie den Missbrauch von IT-Systemen eingegangen.

3.3.1 Kategorisierung des Systemmissbrauchs

Grundsätzlich kann der Systemmissbrauch nach J.P Anderson [And80] in drei Kategorien gruppiert werden. Man unterscheidet hierbei zwischen:

- **Externe Eindringlinge:** Zu dieser Kategorie zählen die diversen Formen von Computereindringlingen, die versuchen, sich von außen unautorisierten Zugriff auf Systeme zu verschaffen, um beispielsweise sensible Daten und Passwörter zu erlangen. Externe Eindringlinge können nochmals in weitere Gruppen unterteilt werden. Jedoch wird in dieser Arbeit anschließend nur auf die Bekanntesten eingegangen. In diesem Kontext soll auch der Begriff der „Hacker“ Erwähnung finden, welcher aber eine sehr allgemeine Bedeutung besitzt. Es handelt sich dabei um Personen, die umfangreiche technische sowie computertechnische Grundlagenkenntnisse besitzen und diese nutzen, um unautorisierten Zugriff auf IT-Systeme und deren Daten zu erlangen. Oftmals liegt ihr Grundgedanke einfach nur darin, aus Langeweile oder zur Selbstbestätigung Angriffe auf Systeme durchzuführen und Schaden anzurichten. Geht man näher ins Detail, kann man nach S.M. Furnell [FUR02] folgende Gruppen unterscheiden:
  - **Cyberterrorists:** sind Personen, welche Techniken anwenden, um Angriffe gegen Systeme, Netzwerke und/oder Daten durchzuführen. Oftmals spielen politische Ansichten beziehungsweise soziale Aspekte für sie eine bedeutende Rolle, mit dem Ziel, eine andere Partei (z.B. Regierungen, Behörden) einzuschüchtern oder zu etwas zu zwingen.
  - **Cyberwarriors:** sind Personen, die mittels Techniken versuchen, Computersysteme anzugreifen, um an unerlässlicher Infrastruktur Schaden anzurichten. Beispiele hierfür wären, Elektrizitätsversorgung, Transport und

Kommunikation, Finanztransaktionen. Cyberwarriors agieren oftmals in Zusammenhang und im Kontext von Militär und Krieg.

- **Malware writers:** sind verantwortlich für die Schaffung von „Malware“-Programmen wie Viren, Würmer und Trojaner. Sie stellen gegenwärtig im Internet eine der größten Gefahren dar, sowohl für den Privatanwender als auch für Unternehmen.
- **Phreakers:** sind jene Gruppe von Personen, die sich darauf spezialisiert haben, Telefonnetzwerke und verwandte Technologien anzugreifen. Ihre Ziele bestehen zum einen darin, die Infrastruktur auszuforschen bis hin zu Manipulation dieser.
- **Script kiddies:** sind Individuen, die im Grunde genommen geringe computertechnische Kenntnisse haben und abhängig von Skripten und Programmgen sind, die von Personen mit größere technischer Kompetenz geschrieben wurden. Jedoch stellen auch sie eine große Gefahrenquelle dar und verursachen mittels ihrer Programme und Skripten, welche über das Internet einfachst verbreitet werden können, enormen Schaden.

- **Interne Eindringlinge:** Hierbei handelt es sich um autorisierte User, oftmals auch Mitarbeiter des eigenen Unternehmens, welche versuchen, auf Teile von Systemen Zugriff zu erlangen, obwohl sie dafür eigentlich keine Berechtigungen besitzen. Diese Art von Eindringlingen unterteilt man nochmals in „Masqueraders“ und „Clandestine Users“. Masqueraders agieren unter der Identität eines anderen Users/Mitarbeiters im System. Dies geschieht einerseits durch Diebstahl des Passworts, oder dadurch, dass Mitarbeiter sich nicht an ihrem Arbeitsplatz befinden und sich nicht aus-geloggt haben. Bei Clandestine User handelt es sich um Personen, die versuchen, Sicherheitsvorkehrungen zu umgehen bzw. zu deaktivieren, um so unautorisierten Zugriff zu erlangen. [FKLP08]

- **Rechtemissbrauch:** diese Art von Missbrauch wird von Personen ausgeübt, welche grundsätzlich autorisiert sind, das System und deren Ressourcen zu nutzen, jedoch ihre Privilegien für andere Zwecke missbrauchen. [FKLP08]

3.3.2 Malware

Bei „Malware“ (Malicious Software) handelt es sich um einen Überbegriff diverser Schadsoftware. Die Schadfunktion der Software ist gewöhnlich getarnt und läuft meist im Hintergrund, unbemerkt vom Benutzer ab. Dadurch stellen sie ein großes Gefahrenpotential für IT-Infrastrukturen von Unternehmen dar, indem sie beispielsweise von Mitarbeitern unbeabsichtigt in das interne Firmennetzwerk eingeschleust werden. [KRA04]

Zu den meistverbreitenden Typen von Malware zählen Viren, Trojaner, Würmer, Spam, Hoaxes und Rootkits.

3.3.3 Wirkung und Konsequenzen eines Sicherheitsbruchs

Wie bereits erwähnt, gibt es eine Vielzahl von kritischen Faktoren, die zu einem Sicherheitsbruch führen können, mit negativen Konsequenzen für Unternehmen und deren IT-Systeme. Nach [FKLP08] können sich die negativen Auswirkungen wie folgt widerspiegeln:

- **Offenlegung:** ist eine häufig eintretende Auswirkung eines Sicherheitsbruchs und hat zur Folge, dass die Vertraulichkeit in ein System nicht mehr gegeben ist, da sensible Informationen und Unternehmensdaten unberechtigt in die Hände von Dritten gelangen können.

- **Verweigerung:** die Verweigerung des Zugriffs auf Daten beeinflusst in großem Ausmaß auch deren Verfügbarkeit, was weitreichende Folgen haben kann.

- **Zerstörung:** diese Form von Sicherheitsbruch hat ebenfalls weitreichende Auswirkungen auf die Verfügbarkeit von Informationen. Ist das Recovery der Daten nicht möglich, kann dies zu enormen Schäden für Unternehmen führen.

- **Veränderung von Systemen und deren Daten:** tritt dieser Bruch ein, ist die Integrität der Daten nicht mehr gewährleistet. Das Problem

liegt darin, dass es oftmals längere Zeit dauert, um diesen Sicherheitsbruch aufzudecken und zu beheben. Dies führt dazu, dass auch hier großer Schaden angerichtet werden kann, wenn dieser Bruch über längere Zeit unbemerkt bleibt.

All diese Auswirkungen eines Sicherheitsbruchs innerhalb eines Unternehmens können ernstzunehmende Konsequenzen haben, die häufig erst nach längerer Zeit offensichtlich werden. Einerseits kann sich ein Sicherheitsbruch sofort in einem finanziellen Verlust für das Unternehmen widerspiegeln, andererseits kann dieser auch schleichend voran schreiten. Oftmals besteht die Gefahr, dass die Reputation eines Unternehmens in Mitleidenschaft gezogen wird, dass sensible Daten in die Hand von Mitbewerbern gelangen, dass Privacy-Rechte verletzt werden oder das Rechtsverfahren gegen das Unternehmen eingeleitet werden. Gravierende Auswirkungen für ein Unternehmen bestehen auch dann, wenn Kerngeschäftsprozesse betroffen sind und diese über einen längeren Zeitraum nicht oder nur eingeschränkt zur Verfügung stehen.

Um Sicherheitsbrüche und die daraus resultierenden Konsequenzen zu vermeiden, gilt es für die Unternehmen, ihre Assets und Risiken genauestens zu identifizieren und bestmöglichen Schutz mittels eines vernünftigen Business-Integrated Information Security Management zu erlangen.

3.4 Ableitung der Zielsetzungen der IT-Security

Zusammenfassend und die bestehenden Risiken, Gefahren, Verwundbarkeiten und Angriffe, die ein IT-System erleiden kann, betrachtend, lassen sich nach [Bis03] folgende drei wesentliche Zielsetzungen ableiten.

- **Schutz (Protection)** eines IT-Systems durch Bereitstellung von Schutzmechanismen. Dieses Ziel beinhaltet das Fehlschlagen von Angriffen.
    - Schlagwörter: Intrusion Detection Systeme (IDS), Firewalls, Back-up Systeme, Ausfallschutz

- Das Ziel des **Nachweises (Detection)** gilt es zu verfolgen, wenn ein Angriff auf ein IT-System bereits stattgefunden hat. Es dient dazu, die Effektivität von Schutzmechanismen aufzuzeigen und im Falle eines Angriffs, diesen zu dokumentieren.

    - Schlagwörter: Intrusion Detection Systeme (IDS), LogFile Analysen, Antivirenscanner

- **Wiederherstellung (Recovery)** umfasst zwei Formen. Die erste Form hat zum Ziel, einen Angriff zu stoppen, diesen zu beurteilen und dementsprechend Konsequenzen daraus zu ziehen, beispielsweise, welche Möglichkeiten es zur Beseitigung dieser Schwachstelle im System gibt. Die zweite Form der Wiederherstellung zielt darauf ab, einen Schaden zu beheben, der durch eine Attacke entstand, obwohl das IT-System grundsätzlich fehlerfrei weiter läuft. Der Unterschied zur ersten Form liegt darin, dass es gilt, einen Schaden zu beheben, obwohl das System eigentlich einwandfrei funktioniert. Die Umsetzung dieses Ziels gilt aber aufgrund der enormen Komplexität heutiger IT-Systeme als sehr schwierig.

    - Schlagwörter: Incident Management, Emergeny-Response Management

Die Autoren des Buchs „Securing Information and Communication Systems“ [FKLP08] sehen die Ziele der IT-Security aus mehreren Perspektiven. Es wird vom Ansatz ausgegangen, dass IT-Security nicht nur eine technologische Herangehensweise benötigt, sondern ein Puzzle aus verschiedenen Perspektiven ist, welche es zu verfolgen gilt. Mit dem Ziel, den Schutz der IT-Security zu gewährleisten, sollten folgende Perspektiven beachtet werden:

- **Technische Perspektive:** hierzu zählen systembasierte Sicherheitsvorrichtungen wie etwa Authentifizierung, Zugangskontrolle, Antivirenschutz und Datenschutz.

- **Physische Perspektive:** bezieht sich auf physische Zugangskontrolle zu Systemen, Schutz vor Diebstahl, Sicherheitsvorrichtungen gegen Feuer, Wasser oder andere umweltbedingte Einflüsse.

- **Personelle Perspektive:** hat den Zweck, adäquate Kontrollen durchzuführen bezüglich der Mitarbeiter, die ein System nutzen. Dies beinhaltet unter anderem ausführliche Bewerbungsgespräche, Security Trainingsprogramme, Schulungen bezüglich dem Sicherheitsbewusstsein der Angestellten; Die Einhaltung von Richtlinien beim Ausscheiden eines Mitarbeiters aus dem Unternehmen, die der ehemalige Angestellte einhalten muss, z.B. Nicht-Veröffentlichung der Security Richtlinie oder das Verbot der Weitergabe vertraulicher firmeninterner Daten.

- **Prozedurale Perspektive:** bezieht sich auf die Notwendigkeit zur Einführung einer Security Richtlinie, Durchführung von Risikoanalysen, aber auch Themen wie Disaster Planning und Disaster Recovery.

- **Rechtliche Perspektive:** bezieht sich auf die Einhaltung rechtlicher Aspekte, wie Datenschutz, Computerkriminalität und Missbrauch.

4 Existierende Planungsansätze der IT-Security

Im folgenden Kapitel wird näher auf die existierenden Planungsansätze im Security Bereich in Unternehmen eingegangen. Es wird darauf eingegangen, welche internationalen Sicherheitsstandards in zahlreichen Unternehmen zum Einsatz kommen, wie zum Beispiel der **ISO/IEC 27001** „Information technology – Security techniques – Information security management systems – Requirements“ und der ISO/IEC 27002 „Information technology -- Security techniques -- Code of practice for information security management“, aber auch die **BSI Grundschutzkataloge**, welche vom deutschen Bundesamt für Sicherheit in der Informationstechnik veröffentlicht werden und dazu dienen, eine einfache Methode bereit zu stellen, die dem Stand der Technik entspricht, um Sicherheitsmaßnahmen zu identifizieren und effizient umzusetzen.

Die Autoren Heinrich Kersten, Gerhard Klett unterscheiden Sicherheitsverantwortliche in den Unternehmen heute in zwei unterschiedliche Gruppen. Während die eine im Schwerpunkt sehr Maßnahmen-orientiert denkt, sieht die andere mehr den Sicherheitsprozess und sein Management im Vordergrund [KK08].

Dies sollte jedoch keinen Gegensatz darstellen, in der Realität ist davon auszugehen, dass man beide Ansätze benötigt, um ein flächendeckendes Sicherheitskonzept zu erstellen. Zurück zu führen ist das zum einen darauf, dass ein Prozess sich international viel leichter standardisieren lässt, als etwa ein Maßnahmenkatalog, der ständig aktualisiert werden muss und bei einer Vielzahl von IT-Anwendungen immer nur Ausschnitte abdeckt. Hierbei wäre der internationale Standard ISO/IEC 27001 anzuführen, welcher aus dem British Standard entstanden ist und die IT-Security im Grunde als einen Managementprozess sieht.

Parallel zu dem ISO/IEC 27001 Standard werden in Deutschland vom BSI die Grundschutzkataloge entwickelt, deren Kern man als maßnahmen-orientiert bezeichnen könnte. Diese Maßnahmenkataloge dienen vor allem im

deutschsprachigen Raum als eine der Grundlagen zur Schaffung von grundlegenden Sicherheitsmechanismen in Unternehmen.

Im folgenden Kapitel der Arbeit wird sowohl auf das IT-Sicherheitsmanagement nach ISO 27001 eingegangen, als auch auf das IT-Grundschutzhandbuch des deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI). Zudem wird auch kurz das **österreichische Informationssicherheitshandbuch** beschrieben, welches sich aber größtenteils nach den internationalen Vorgaben der ISO/IEC 27000 Normreihe und auch der IT-Grundschutz-Vorgehensweise des BSI orientiert. Zum Ende dieses Abschnitts wird im letzten Unterkapitel noch auf den **Common Criteria (CC) Ansatz** eingegangen, welcher als international anerkannter Standard zur Bewertung der Sicherheit von Informationstechnologie dient.

4.1 Securitykonzept nach ISO/IEC 27001

Ein heute weit verbreiteter Ansatz zur Erstellung eines ausgereiften Securitykonzepts ist das Vorgehen nach dem ISO/IEC 27001 Standard. Der Standard dient zur Spezifikation der Anforderungen für die Herstellung, Einführung, Betrieb, Überwachung, Pflege und Verbesserung eines dokumentierten Informationssicherheitsmanagementssystems (ISMS) unter Berücksichtigung der Risiken innerhalb der gesamten Organisation eines Unternehmens [ISO10].

Der Vorteil des ISO/IEC Standards liegt darin, dass er auf alle Bereiche angewandt werden kann, seien es Handelsunternehmen, Regierungsbehörden oder auch einfach nur Non-profit Unternehmen. Er ermöglicht, dass unter der Auswahl und Verwendung der geeigneten Sicherheitsmaßnahmen sämtliche Werte entlang der Wertschöpfungskette eines Unternehmens effizient geschützt werden.

Bei der Entwicklung des ISO/IEC 27001 Standards hatte man die Absicht, diesen so zu entwerfen, dass er für verschiedene Anwendungsgebiete geeignet ist. Um die vielseitigen Verwendungsmöglichkeiten des Standards für

Unternehmen aufzuzeigen, werden nachstehend einige der Wichtigsten aufgelistet [Bre07]:

- Zur **Formulierung** von **Sicherheitsanforderungen** und **Zielen** innerhalb einer Organisation
- Um zu garantieren, dass **Sicherheitsrisiken kosten-effektiv gemanagt** werden können
- Als ein **Prozessframework** zur **Implementierung** und zum **Management** von **Kontrollmechanismen**, um gewährleisten zu können, dass Sicherheitsanforderungen und Ziele eingehalten werden
- Zur **Identifikation** bestehender **Information Security Management Prozesse**, aber auch zur **Definition** von neuen
- Um relevante Informationen über **Security Policies, Standards** und **Methoden** der Organisation für Handelspartner und andere Unternehmen zur **Verfügung** zu stellen, welche aus operativen oder kommerziellen Gründen miteinander interagieren

4.1.1 Umsetzung eines ISMS nach ISO 27001

Die Umsetzung zur Einführung und der Betrieb eines ISMS nach dem ISO 27001 Standard erfolgt nach einem prozessorientierten Ansatz, welchem das Plan-Do-Check-Act-Modell (PDCA) zu Grunde liegt [ISO10]. Dadurch kann die Skalierbarkeit eines ISMS gewährleistet werden, und es bietet sich die Möglichkeit zur ständigen Anpassung und Verbesserung. Beim PDCA-Modell handelt sich um ein 4-Phasenmodell (siehe Abbildung 5: PDCA-Zyklus nach [KRS09]) aus einer sich zyklischen wiederholenden Abfolge von Tätigkeiten, derer sich ein Unternehmen bedienen sollte, solange es ein ISMS betreibt [KRS09].

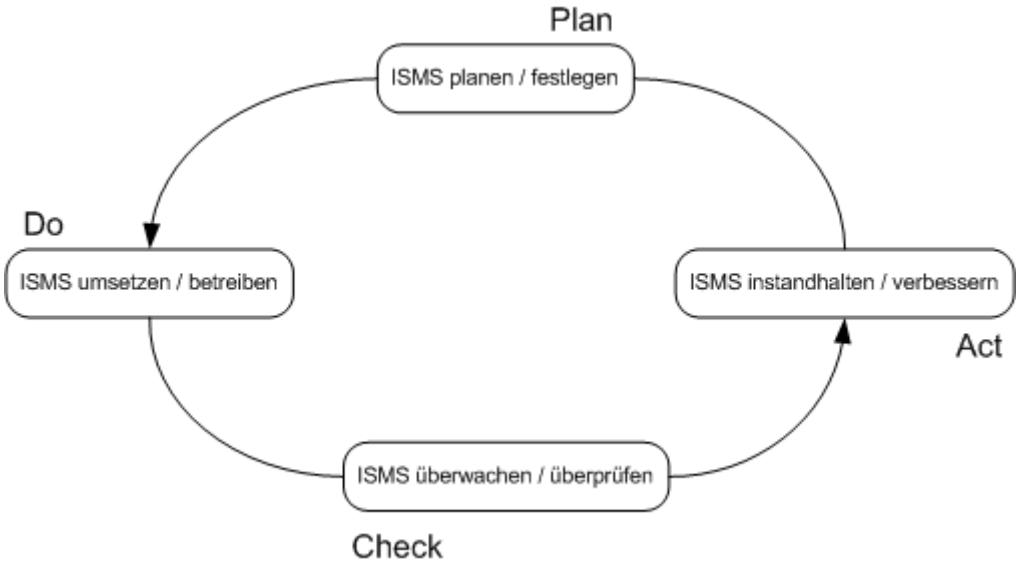


Abbildung 5: PDCA-Zyklus nach [KRS09]

In weiterer Folge werden die einzelnen Phasen in Anlehnung an den ISO 27001 Standard überblicksmäßig beschrieben.

Plan: Das ISMS festlegen

Dem ersten Zyklus des PDCA-Modells liegen zwei unterschiedliche Zwecke zugrunde. Zum einem die Planung eines noch nicht existierenden ISMS und zum anderen die Anpassung eines bereits existierenden ISMS an veränderte Gegebenheiten. Die Vorgehensweise orientiert sich in beiden Fällen am Abschnitt 4.2.1 des ISO 27001 Standards. Anhand eines kurzen Leitfadens werden die wichtigsten Schritte zur Planung eines ISMS überblicksmäßig beschrieben [ISO10]:

a) Bei der Planung werden im ersten Schritt der Anwendungsbereich und die Grenzen des ISMS festgelegt.
b) Definition der ISMS- und Informationssicherheitsrichtlinie; In der Informationssicherheitsrichtlinie werden gesetzliche, vertragliche und andere regulative Anforderungen, sowie die Verpflichtung aller Mitarbeiter zur Einhaltung dieser festgelegt. Zusätzlich werden in der

Leitlinie Rahmenbedingungen zur Erreichung der Informationssicherheit festgelegt [KRS09]. Ebenso wird festgelegt, in welcher Form Risiken für das Unternehmen zu bewerten sind. Die Freigabe erfolgt durch das Management.

c) Anschließend erfolgt eine Identifizierung der Risiken und deren Bewertung
d) Es werden Maßnahmenziele und Maßnahmen festgelegt. Der ISO 27001 Standard beinhaltet im Anhang A ein Paket aus schon bereitgestellten Maßnahmenzielen und Maßnahmen, die von Unternehmen umgesetzt werden können.

Sind all diese Aufgaben erfüllt, kann der Auftrag zur Einführung des ISMS gegeben werden. Hierbei muss ein Dokument zur Erklärung der Anwendbarkeit des ISMS angefertigt werden, welches auch als „Statement of Applicability“ (SoA) bezeichnet wird [KRS09].

Do: Umsetzen und Betreiben des ISMS

Diese Phase im PDCA-Zyklus dient zum Aufbau eines funktionierenden ISMS. Die Umsetzung orientiert sich abermals an dem ISO 27001 Standard [ISO10], Kapitel 4.2.2.:

a) Zu Beginn wird ein Risikobehandlungsplans formuliert, bei dem es sich aber nicht um Planungsaktivitäten handelt, sondern um Ausführung bzw. Umsetzung. Es wird festgelegt, wie mit Risiken umgegangen werden soll und welche Aktionen und Ressourcen erforderlich sind, um den Risiken entsprechend entgegenwirken zu können. Eine geeignete Handlung wäre beispielsweise die Inbetriebnahme der ISMS-Leitlinie, sowie die Vermittlung der enormen Bedeutung, die sie für das Unternehmen besitzt [KRS09].
b) Im nächsten Schritt erfolgt die Umsetzung des Risikobehandlungsplans und der Maßnahmenziele.

c) Überprüfen, ob die Resultate der Einzelmaßnahmen zum Erreichen der Maßnahmenziele führen
d) Sensibilisieren und Schulen der Mitarbeiter bezüglich der ISMS
e) Verwaltung des Betriebs des ISMS
f) Erkennung und Management von Sicherheitsvorfällen

Check: Überwachen und Überprüfen des ISMS

Diese Phase im PDCA-Zyklus dient der Überwachung und der Steuerung eines funktionierenden ISMS und entspricht dem Kapitel 4.2.3 des ISO 27001 Standards [ISO10]:

a) Bei der Überwachung und der Überprüfung sollen Fehler in der Datenverarbeitung erkannt werden. Es werden Indikatoren festgelegt, um etwaige Vorfälle rechtzeitig zu erkennen und in weiterer Folge zu verhindern
b) Es erfolgt eine regelmäßige Überprüfung der Wirksamkeit des ISMS. Dies wird durch die Einhaltung der ISMS-Leitlinie, das Erreichen der Sicherheitsziele, sowie durch die gezielten Maßnahmen garantiert. Im Rahmen einer Managementbewertung wird die Wirksamkeit des ISMS überprüft. Hier fließen Erkenntnisse aus Sicherheitsaudits, früheren Bewertungen und Rückmeldungen aus der Praxis ein. Darüber hinaus wird geprüft und dokumentiert, inwiefern Maßnahmen noch ihrer Wirksamkeit entsprechen und ob etwaige Anpassungen notwendig sind.
c) Ein weiterer wichtiger Punkt in dieser Phase sind sich wiederholende Risikoeinschätzungen, aufgrund veränderter Geschäftsziele und Prozesse, sowie die Durchführung interner Audits um die Defizite des ISMS aufzuzeigen.
d) Managementbewertungen des ISMS und Aktualisierung des Incident Managementplans fallen ebenfalls in diese Phase.

Act: Pflegen und Verbessern des ISMS

Die letzte Phase des PDCA-Zyklus dient zur Pflege und Verbesserung des ISMS und entspricht wiederum dem Abschnitt 4.2.4 der ISO 27001 Normierung [ISO10]:

a) Identifizierte Verbesserungen der Check-Phase werden umgesetzt

b) Korrektur und Vorbeugemaßnahmen dienen dazu, um nicht wirksame Maßnahmen zu korrigieren oder durch andere zu ersetzen. Es werden Vorbeugemaßnahmen getroffen, um Sicherheitsvorfälle schon im Voraus zu verhindern. Ebenfalls können Informationen aus anderen Unternehmen derselben Branche einfließen, um das ISMS zu verbessern.

c) Die geplanten bzw. durchgeführten Verbesserungen müssen an die Mitarbeiter kommuniziert und ständig kontrolliert werden, um die Wirksamkeit der Maßnahmen zu prüfen.

Weiters muss noch erwähnt werden, dass parallel zu allen wichtigen Entscheidungen der vier Phasen eine ausführliche Dokumentation vorausgesetzt wird (siehe Kapitel 4.3. des Standards [ISO10]), auf die in dieser Arbeit aber nicht näher eingegangen wird.

4.2 IT-Grundschutzkataloge

Ein weiterer ganzheitlicher Ansatz, um die Basissicherheit in Unternehmen zu gewährleisten, speziell im deutschsprachigen Raum sind die IT-Grundschutzkataloge, welche vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) publiziert werden. Aufgrund ihres internationalen Anklangs und ausführlichen Ausarbeitung werden die Kataloge auch in digitaler Form in englischer Sprache zur Verfügung gestellt. Dies ist auch ein wesentlicher Grund, wieso die Kataloge in dieser Arbeit Berücksichtigung finden. Sie dienen dazu, Sicherheitsverantwortliche in der Identifikation und der Umsetzung von geeigneten Sicherheitsmaßnahmen für Unternehmen zu unterstützen. Mittels der Kombination aus der IT-Grundschutz-Vorgehensweise

(BSI-Standard 100-2) und den IT-Grundschutz-Katalogen (Baustein-, Maßnahmen- und Gefährdungskataloge stellt das BSI für die verschiedensten Einsatzumgebungen Maßnahmen zum sicheren Umgang mit Informationen zur Verfügung, sowohl eine Sammlung von geeigneten Sicherheitsmaßnahmen als auch eine entsprechende Methodik zur Auswahl und Anpassung dieser [BSI09]. Bereitgestellte Mechanismen umfassen gewisse Standards für Geschäftsprozesse, Anwendungen und IT-Systeme mit „normalem“ Schutzbedarf, sowie eine Darstellung der pauschal angenommenen Gefährdungslage und daraus resultierende ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe, um einen angemessenen Basisschutz für alle Assets eines Unternehmens zu erreichen.

Die IT-Grundschutzkataloge basieren auf einem Baukastenprinzip, was heißt, dass die einzelnen Bausteine beispielsweise typische Abläufe von Geschäftsprozessen und Bereichen, wo IT-Einsatz erforderlich ist widerspiegeln. Jeder Baustein wird zum einem durch die zu erwartende Gefährdungslage beschrieben, welche als Grundlage für ein entsprechendes Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge dient.
Den Vorteil sehen die Macher der IT-Grundschutzkataloge in der Vereinfachung und möglichst ökonomischen Erstellung eines Sicherheitskonzepts. Für jeden Baustein gibt es vorgefertigte Risikoanalysen, um vorab die Bedrohungen und deren Eintrittswahrscheinlichkeiten zu ermitteln und um in weiterer Folge die passenden Sicherheitsmaßnahmen auszuwählen, um schlussendlich das verbleibende Restrisiko bewerten zu können.
Durch die Anwendung der IT-Grundschutzkataloge in einem Unternehmen reduziert sich die Analyse auf einen Soll-Ist-Vergleich zwischen den empfohlenen und den bereits realisierten Sicherheitsmaßnahmen. Dadurch lassen sich fehlende oder noch nicht umgesetzte Maßnahmen leicht erkennen und es werden die Sicherheitsdefizite aufgezeigt, die es zu beheben gilt. Die IT-Grundschutzkataloge setzen ein gewisses Maß an vorhandenem

Sicherheitsbewusstsein in einem Unternehmen voraus, was heißt, dass bei Vorliegen von gravierenden Sicherheitsmängeln ergänzende Sicherheitsanalysen über die IT-Grundschutzkataloge hinaus notwendig sind. Dafür verweist das Bundesamt für Sicherheit in der Informationstechnik auf den von ihr publizierten Standard „Risikoanalyse auf der Basis von IT-Grundschutz“ (BSI-Standard 100-3) [BSI09].

Um die Maßnahmenempfehlungen leichter umsetzbar zu machen, sind die Sicherheitsmaßnahmen in verschiedene Kataloge unterteilt und dort im Detail beschrieben. Weiters werden zur Realisierung der Maßnahmen, um einen Basisschutz an Sicherheit zu gewährleisten, Hilfsmittel und Musterlösungen vom BSI und anderen IT-Grundschutzanwendern zur Verfügung gestellt.
Darüber hinaus zeichnen sich die Maßnahmenkataloge des IT-Grundschutz dadurch aus, dass sie auf ständige Aktualisierbarkeit und Erweiterbarkeit ausgelegt sind. Dies ist durchaus von großem Vorteil, wenn man bedenkt, wie innovativ die IT-Branche ist und das Unternehmen darüber hinaus ständig mit neuen Herausforderungen konfrontiert sind, um ein gewisses Maß an Sicherheit zu bewahren.

4.2.1 Aufbau der IT-Grundschutzkataloge

Im folgenden Kapitel wird ein grober Überblick über den Aufbau der IT-Grundschutzkataloge gegeben, sowie ein systematischer Weg, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet werden kann.

Kataloge	**Beschreibung**
Bausteine	Enthalten Kurzbeschreibungen der betrachteten Komponenten, Vorgehensweisen und IT-Systeme. Geben einen Überblick über die Gefährdungslage und Maßnahmenempfehlungen
Gefährdungskataloge	Enthalten detaillierte Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen

	genannt wurden
Maßnahmenkataloge	Enthalten die detaillierte Beschreibung der Sicherheitsmaßnahmen bzw. Maßnahmenempfehlungen aus den einzelnen Bausteinen

Bausteine:

B1	Übergreifende Aspekte der Informationssicherheit. Diese Schicht ist des Weiteren in kleinere Bausteine (B1.0 bis B1.14) unterteilt
B2	Sicherheit der Infrastruktur Diese Schicht ist des Weiteren in kleinere Bausteine (B2.1 bis B2.12) unterteilt
B3	Sicherheit der IT-Systeme Diese Schicht ist des Weiteren in kleinere Bausteine (B3.1xx bis B3.4xx) unterteilt
B4	Sicherheit im Netz Diese Schicht ist des Weiteren in kleinere Bausteine (B4.1 bis B4.7) unterteilt
B5	Sicherheit in Anwendungen Diese Schicht ist des Weiteren in kleinere Bausteine (B5.1 bis B5.16) unterteilt

Die Bausteine sind der zentrale Bestandteil der IT-Grundschutzkataloge.

Gefährdungskataloge:

G1	Höhere Gewalt Diese Schicht ist des Weiteren in kleinere Bausteine (G1.1 bis B1.17) unterteilt
G2	Organisatorische Mängel Diese Schicht ist des Weiteren in kleinere Bausteine (G2.1 bis G2.140)

	unterteilt
G3	Menschliche Fehlhandlungen Diese Schicht ist des Weiteren in kleinere Bausteine (G3.1 bis G3.92) unterteilt
G4	Technische Versagen Diese Schicht ist des Weiteren in kleinere Bausteine (G4.1 bis G4.71) unterteilt
G5	Vorsätzliche Handlungen Diese Schicht ist des Weiteren in kleinere Bausteine (G5.1 bis G5.145) unterteilt

Maßnahmenkataloge:

M1	Infrastruktur Diese Schicht ist des Weiteren in kleinere Bausteine (M1.1 bis M1.69) unterteilt
M2	Organisation Diese Schicht ist des Weiteren in kleinere Bausteine (M2.1 bis M2.430) unterteilt
M3	Personal Diese Schicht ist des Weiteren in kleinere Bausteine (M3.1 bis M3.66) unterteilt
M4	Hard- und Software Diese Schicht ist des Weiteren in kleinere Bausteine (M4.1 bis M4.324) unterteilt
M5	Kommunikation Diese Schicht ist des Weiteren in kleinere Bausteine (M5.1 bis M5.150) unterteilt
M6	Notfallvorsorge Diese Schicht ist des Weiteren in kleinere Bausteine (M6.1 bis M6.109) unterteilt

4.2.2 Systematischer Weg zur Umsetzung eines funktionierenden ISMS

Die IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) beschreibt die diversen Aktivitäten innerhalb eines Unternehmens und deren Zusammenhang zu den Maßnahmen, die es zur Umsetzung eines Sicherheitskonzepts zu bewerkstelligen gilt.

Im ersten Schritt geht es um die Festlegung bzw. Identifizierung der Rollen, welche für die Initiierung bzw. Umsetzung eines Sicherheitskonzepts und der Sicherheitsmaßnahmen verantwortlich sind.

Exemplarisch könnte eine mögliche Rollenfestlegung nach [BSI10] wie folgt aussehen:

- **IT-Sicherheitsbeauftragter:** gibt die Informationssicherheitsleitlinie in Absprache mit der Unternehmensführung vor. Ist als Koordinator, sowie Hauptansprechpartner für Fragen bei der Erstellung eines Informationssicherheitskonzepts zuständig
- **Informationssicherheitsverantwortliche bzw. IT-Administratoren:** sind für die Pflege und Wartung von IT-Systemen und Anwendungen verantwortlich. Des Weiteren sind sie für die technische Umsetzung von festgelegten Maßnahmen zuständig.
- **Mitarbeiter:** umfassen alle anderen Angestellten eines Unternehmens. Können je nach Bedarf diverse Tätigkeiten vom IT-Sicherheitsbeauftragten erteilt bekommen und unterstützen diesen bei der Erstellung des Sicherheitskonzepts.

Erstellung des Sicherheitskonzepts in 7 Phasen, angelehnt an [BSI10]:

	Phase	**Beschreibung**	**Beteiligte Akteure**	**Output**
1	Initiierung des Sicherheitsprozesses	Definition des Geltungsbereichs des Informationsverbunds. Erstellung der Leitlinie zur Informationssicherheit. Wenn nötig, Planung und Einrichtung einer IT-Sicherheitsorganisation.	IT-Sicherheitsbeauftragter	Leitlinie zur Informationssicherheit
2	Durchführung einer Strukturanalyse	Analyse aller Komponenten eines Informationsverbunds (Anwendungen, IT-Systeme, Kommunikationsverbindungen usw.).	IT-Sicherheitsbeauftragter und Mitarbeiter)	Überblick über die IT-Landschaft, Standorte, Benutzer und Verantwortliche
3	Durchführung einer Schutzbedarfserstellung	Anpassung der Schutzbedarfskategorien auf den Informationsverbund. Einbeziehung der Mitarbeiter, da diese den Schutzbedarf oftmals sehr gut einschätzen können.	IT-Sicherheitsbeauftragter und Mitarbeiter)	Für alle analysierten Komponenten aus Phase 2 wurde der Schutzbedarf festgelegt
4	Modellierung nach IT-Grundschutz	Informationsverbund wird mittels der Bausteine aus den IT-Grundschutzkatalogen nachgebildet.	IT-Sicherheitsbeauftragter und Sicherheitsverantwortliche	IT-Grundschutzmodell
5	Durchführung des Basis-Sicherheitschecks	Kontrolle, inwieweit Sicherheitsmaßnahmen, die während der Modellierung ermittelt wurden, schon oder noch nicht im Unternehmen umgesetzt wurden	Sicherheitsbeauftragter und Sicherheitsverantwortliche	Sicherheitscheck gibt Auskunft über den Umsetzungsstatus der geforderten Basis-

				Sicherheitsmaßnahmen
6	Realisierung von Sicherheitsmaßnahmen	Erforderliche Sicherheitsmaßnahmen werden umgesetzt. Erstellung eines Realisierungsplans zur Umsetzung der Maßnahmen, welche essentiell sind und ob gegebenenfalls auf einige verzichtet werden kann.	IT-Sicherheitsbeauftragter mit Arbeitsgruppe	Realisierungsplan und umgesetzte Maßnahmen
7	Aufrechterhaltung der Sicherheit und kontinuierliche Verbesserung der Informationssicherheit	Laufende Überprüfung des Informationssicherheitsprozesses auf Effektivität und Effizienz, um so auf etwaige Zwischenfälle entsprechend reagieren zu können.	Sicherheitsbeauftragter und Sicherheitsverantwortliche	
8	Zertifizierung	Grundschutzsicherheitskonzept auf Basis des ISO 27001 Standards zertifizieren lassen	IT-Sicherheitsbeauftragter	

4.3 Österreichisches Informationssicherheitshandbuch

Das österreichische Informationssicherheitshandbuch stellt einen weiteren Ansatz zur Etablierung eines umfassenden Informationssicherheits-Managementsystems dar. Für die Erstellung des Handbuchs zeichnen sich drei Kooperationspartner aus. Dabei handelt es sich um Das Bundeskanzleramt Österreich (BKA), das Informatikstrategieorgan des Bundes (ISB) aus der Schweiz und das Zentrum für sichere Informationstechnologie – Austria (A-SIT), als Projektverantwortlicher. [BKÖ10]

Der Aufbau und Inhalt des Sicherheitshandbuches orientiert sich größtenteils nach den internationalen Vorgaben der ISO/IEC 27000 Normreihe und auch der IT-Grundschutz-Vorgehensweise des BSI. Auszeichnen soll es sich laut den Autoren durch seine internationale Ausrichtung und Kompaktheit. Darüber hinaus soll es einen wesentlichen Beitrag zur Erstellung und Implementierung von umfangreichen Sicherheitskonzepten in der öffentlichen Verwaltung leisten und auch als Hilfestellung für die Wirtschaft dienen[BKÖ10].

Da sich das österreichische Informationssicherheitshandbuch zum größten Teil an der ISO/IEC 27000 Normreihe orientiert und die Erstellung in Kooperation mit dem BSI erfolgte, wird in dieser Arbeit nicht näher auf den Aufbau eingegangen, um Wiederholungen zu vermeiden.

4.4 Common Criteria for Information Technology Security Evaluation

Der Common Criteria (CC) Ansatz dient zur Bewertung der Sicherheit von Informationstechnologie. Beim CC handelt es sich um eine internationale Norm, um die Datensicherheit von Computersystemen zu zertifizieren. Die Entwicklung der Norm geht auf die Zusammenarbeit von verschiedenen Partnern aus verschiedenen Ländern zurück und vereint die Stärken diverser anderer Standards. Das “Trusted Computer System Evaluation Criteria (TCSEC)” entwickelt in den USA, als auch das „Information Technology Security Evaluation Criteria (ITSEC)“ initiiert in Europa, fließen in den CC

Ansatz sein. Durch die Einführung des „Arrangement on the Recogination of the Common Criteria Arrangement (CCRA)“ im Jahr 1998 schaffte man es bis heute, einen weltweit anerkannten de-facto- Standard bezüglich der Datensicherheit von Computersystemen zu schaffen. Darüber hinaus ist der CC auch Standard der Norm 15408 der „International Standard Organisation (ISO)“ [BIS03].

Die CC Philosophie ist es, die Vertrauenswürdigkeit eines IT-Produkts sicherzustellen. Dies erfolgt anhand von Bewertungen, welche durch aktive Untersuchungen und Erhebungen durchgeführt wird [CC-3-09].

4.4.1 Aufbau des CC Ansatzes

Der CC Ansatz setzt sich aus drei unterschiedlichen, aber zusammenhängenden Teilen zusammen. Im [CC-1-09] sind sie wie folgt beschrieben:

- **Einführung und allgemeines Modell:** In diesem Teil werden die Konzepte und Prinzipen zur IT-Security Bewertung definiert, sowie ein allgemeines Modell für die Bewertung vorgestellt.
- **Funktionale Sicherheitskomponenten:** In diesem Bereich des CC werden die Komponenten vorgestellt, die die funktionalen Sicherheitsanforderungen für Zielobjekte beinhalten. Ein Zielobjekt kann beispielsweise Software oder auch Hardware sein. Die Gliederung der Komponenten erfolgt in Klassen und Familien.

  Jede Klasse spielgelt einen bestimmten Ansatz bzw. Absicht wider, um ein Sicherheitsziel zu erfüllen. Eine Klasse setzt sich aus mehreren Familien zusammen. Diese wiederum beinhalten detaillierte Beschreibungen und Definitionen von bestimmten Anforderungen [BIS03]. Mittels der diversen Klassen und deren Familien können „Protection Profiles (PP)“ erstellt werden, welche die funktionalen Sicherheitsanforderungen an ein Zielobjekt (z.B. Firewall,

Softwareapplikation) erkenntlich machen [CC-2-07]. In Tabelle 1 sieht man eine Zusammenfassung der Klassen des CC.

Kürzel	Klasse	Kürzel	Klasse
FAU	Sicherheitsprotokollierung	FPR	Privatsphäre
FCO	Kommunikation	FPT	Schutz der Sicherheitsfunktionen
FCS	Kryptographische Unterstützung	FRU	Betriebsmittelnutzung
FDP	Schutz der Benutzerdaten	FTA	Schnittstelle
FIA	Identifikation und Authentisierung	FTP	Vertrauenswürdiger Pfad
FMT	Sicherheitsmanagement		

Tabelle 1: CC Klassen nach [CC-2-07] und [BIS03]

- **Vertrauenswürdigkeit der Sicherheitskomponenten:** Der dritte Teil besteht aus einer Sammlung von Komponenten, welche auf die Anforderungen an die Vertrauenswürdigkeit eines Zielobjekts abzielen. Diese Komponenten werden ebenfalls in Familien und Klassen eingeteilt. Weiters wird eine Sammlung an Bewertungskriterien für implementierungsabhängige und unabhängige Anforderungen an ein Zielobjekt definiert. Ferner wird der Evaluation Assurance Level (EAL) vorgestellt, welcher beispielsweise die Vertrauenswürdigkeit bzw. die Korrektheit einer Implementierung beschreibt (siehe Tabelle 2).

EAL Kürzel	Bedeutung
EAL1	funktionell getestet
EAL2	Strukturell getestet
EAL3	Methodisch getestet und überprüft

EAL4	Methodisch entwickelt, getestet und durchgesehen
EAL5	Semiformal entworfen und getestet
EAL6	Semiformal verifizierter Entwurf und getestet
EAL7	Formal verifizierter Entwurf und getestet

Tabelle 2: Evaluation Assurance Levels nach [CC-3-09]

4.4.2 Evaluierung nach CC

Die Durchführung eines IT-Security Evaluierungsprozesses, welcher dem CC Ansatz entspricht, erfolgt mittels der „Common Methodology for Information Technology Security Evaluation (CEM)“. Das Zielpublikum der CEM sind Bewertungs- und Zertifizierungsorganisationen. Jedoch sollen durch CEM auch Interessensgruppen angesprochen werden, deren Fokus auf IT Security liegt.

Mittels CEM wird ein Minimum an Maßnahmen festgelegt, welche es einer Zertifizierungsautorität erlaubt, eine korrekte Bewertung nach CC durchzuführen [CEM09]. Für den deutschsprachigen Raum führt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Zertifizierung von Produkten (Systeme oder Komponenten) nach CC durch. Im Rahmen eines Zertifizierungsprozesses wird eine technische Prüfung (Evaluierung) durchgeführt. Diese Evaluierung kann nur durch vom BSI anerkannte Prüfstellen erfolgen. Die Ergebnisse eines Zertifizierungsverfahrens werden in einem abschließenden Report festgehalten. Dieser enthält die sicherheitstechnische Beschreibung des zertifizierten Produkts, Einzelheiten der Bewertung, sowie Hinweise für den Anwender [BSI]. Darüber hinaus wird das Produkt noch mit einem EAL Rating von 1-7 ausgezeichnet [BIS03]. Nähere Informationen bezüglich der Zertifizierungsorganisationen, die eine Evaluierung nach CC durchführen, können auf folgender Homepage http://www.commoncriteriaportal.org/ entnommen werden.

4.5 Wissenschaftliche Planungsansätze der IT-Security

Derzeit widmen sich wissenschaftliche Forschungsaktivitäten nicht unbedingt der Schaffung komplett neuer Planungsansätze der IT-Security. Allerdings ist die Tendenz erkennbar, bestehende Planungsansätze zu verbessern. Dazu gibt es einen äußerst interessanten Forschungsbereich, die Automatisierung der Information Security.

In den nachstehenden Kapiteln wird der aktuelle Forschungsstand zum Thema der Automatisierung näher erläutert.

4.5.1 Automatisierung der Information Security

Die Autoren in [FM11] beschreiben das Thema des Information Security Management als ein sehr komplexes aber unbedingt notwendiges Instrument, um die Vertraulichkeit, Integrität und Verfügbarkeit von essentiellen Unternehmensdaten zu garantieren. Dabei hat sich herausgestellt, dass die Umsetzung eines ISMS beispielsweise anhand des ISO 27001 Standards teilweise sehr umfangreich werden kann, überhaupt, wenn versucht wird, eine Compliance bezüglich des Standards zu erreichen. Dazu müssen nach [FM11] über 130 sogenannte „Controls“ implementiert, betrieben und monitored werden. Unter Controls bzw. Maßnahmen nach [ISO08] versteht man:

„Hilfsmittel für das Managen von Risiken, einschließlich Politik und Anweisungen, Verfahren, Richtlinien, Praktiken oder Organisationsstrukturen, die ihrem Wesen nach administrativer, technischer, managementgebundener oder rechtlicher Natur sein können“

Dieser Fakt im Zusammenhang mit der rapiden Technologieweiterentwicklung, die unterschiedliche Ausrüstung, die Unternehmen nutzen, und der Vielzahl von Systemen und Applikationen, die zum Einsatz kommen zeigt, dass eine Automatisierung in Information Security aus Sicht der Autoren für die Zukunft unerlässlich werden wird. [FM11] Bisweilen gibt es zwar Standards in der Entwicklung, welche aber nur auf die Interoperabilität zwischen Applikationen fokussiert sind. Dazu zählt das in [MA09] und [RK11] beschriebene Security

Content Automation Protocol (SCAP), welches im nachfolgenden Kapitel kurz beschrieben wird.

Wie bereits öfters in dieser Arbeit beschrieben, stellen nicht nur die Technologie an sich, sondern auch Personen, Prozesse wichtige Assets und Risikofaktoren bezüglich der IT-Security dar. Dies wiederum impliziert, dass nicht jeder Sicherheitsmanagementaspekt automatisiert werden kann. Unter Automatisierung von Controls bzw. Maßnahmen verstehen [FM11] die Durchführung einer Operation ohne Eingriff einer Person in den Prozess. Die Maßnahme des Awarenesstrainings, bei der Menschen an der Umsetzung beteiligt sind, kann beispielsweise nicht automatisiert werden.

In Abbildung 6: ISO 27001 automatisierbare Kontrollziele nach [FM11] sieht man eine Auswertung hinsichtlich der Automatisierungsmöglichkeit der Controls des ISO 27001 Standards. Für jede der 11 Domänen des Standards wurde die Anzahl der zu automatisierenden Maßnahmen untersucht. Schlussendlich kamen sie im Rahmen ihrer Forschungsaktivitäten zu dem Ergebnis, dass momentan 37 Kontrollziele automatisiert werden können, was 27,8% entspricht.

Domain	**Information Security Controls**			
	Controls that can be automated	*Total controls*	*Percent*	*Examples of controls*
Security policy	0	2	0	-
Organization of information security	0	11	0	-
Asset management	1	5	20%	Inventory of assets
Human resources security	1	9	11.1%	Removal of access rights
Physical and environmental security	2	13	15.4%	Physical entry controls
Communications and operations management	15	32	46.9%	Controls against malicious code
				Information back-up
				Audit logging
Access control	13	25	52%	Unattended user equipment
				Network connection control
Information systems acquisition, development and maintenance	4	16	25%	Key management
				Control of technical vulnerabilities
Information security incident management	0	5	0	-
Business continuity management	0	5	0	-
Compliance	1	10	10%	Technical compliance checking

Abbildung 6: ISO 27001 automatisierbare Kontrollziele nach [FM11]

Grundsätzlich lässt sich aus den Ergebnissen der Studie folgern, dass eine zunehmende Automatisierung hinsichtlich der existierenden Planungsansätze der IT-Security auf alle Fälle wünschenswert wäre, da aktuell ihre vollständige Umsetzung ohne Zuhilfenahme von unterstützenden Tools doch ziemlich zeitintensiv sein kann. Darüber hinaus würde eine Reduktion menschlicher Eingriffe auch eine Kostenersparnis und Reduzierung der Komplexität mit sich bringen.

Darüber hinaus gilt in diesem Zusammenhang auch, darauf hinzuweisen, dass sich die Autoren in [FM11] auf unterschiedliche Tools [Microsoft: Systems Management Server (SMS) and Active Directory (AD); nCircle: IP360 and Configurations Manager (CCM), AlienVault: Open Source Security Information Management (OSSIM), Symantec: Protection Suite Enterprise edition (ED); etc.] stützen, die zur vollständigen Automatisierung aller Controls notwendig wären. Somit gilt es auch zu hinterfragen, inwiefern diese Tools dem Kosten-Nutzen-Faktor für Unternehmen entsprechen und ob diese tatsächlich für den Zweck der Automatisierung ausgereift sind.

Die vollständige Automatisierung aus heutiger Sicht, welche 27,8% der Controls des ISO 27001 Standards entspricht, verlangt somit, dass man zusätzlich diverse Tools einsetzt, da es kein einziges gibt, welches den ganzen Bereich der zu automatisierenden Controls für sich allein abdeckt. Ob diese Tools untereinander kompatibel sind, ist schwer zu beurteilen und müsste genauer analysiert werden. Allerdings setzt sich das bereits erwähnte Security Content Automation Protocol (SCAP) genau mit der Herausforderung der Schaffung von mehr Interoperabilität zwischen Security-Tools auseinander [FM11-1].

Zum derzeitigen Zeitpunkt wird sich der Einsatz von Automatisierungstools, wenn überhaupt, wahrscheinlich nur für größere Unternehmen lohnen. Dennoch sollte man diesen Bereich in Zukunft nicht außer Acht lassen, da hier viel Potential für eine effektivere Gestaltung der IT-Security vorhanden ist.

4.5.2 The Security Content Automation Protocol (SCAP)

Ein weiterer bedeutender wissenschaftlicher Ansatz in Bezug auf die Automatisierung der Information Security fokussiert sich auf die Standardisierung der Formate und der Nomenklatur, über welche Softwareprodukte ihre Informationen bezüglich der Softwareidentifikation, Softwareschwachstellen und Sicherheitskonfigurationen kommunizieren. Diese Anstrengungen resultierten in der Definition des Security Content Automation Protocol (SCAP), welches vom National Institute of Standards and Technology (NIST) der USA initiiert und in Zusammenarbeit mit anderen Organisationen erarbeitet wurde.

Grundgedanke dieses Ansatzes war es, die Defizite wie die fehlende Interoperabilität zwischen den diversen Securitylösungen die in Unternehmen zum Einsatz kommen, zu schließen und Inkonsistenzen in Ergebnissen von Reports zu vermeiden.

Ein Beispiel dafür wäre, dass Tools (z.B. Verwundbarkeitsscanner) proprietäre Namen für Verwundbarkeiten oder Plattformen verwenden, was als Konsequenz bei Auswertungen zu unterschiedlichen Resultaten führt und einen Vergleich schwer möglich macht. Diese Tatsache kann zu Verzögerungen in der Beurteilung des derzeitigen Sicherheitsniveaus, in der Bewertung von Verwundbarkeiten und der Entscheidungsfindung von Maßnahmen führen. [QSBJ11]

Durch die Entwicklung des SCAP verspricht man sich neben einer Zeitersparnis bei der Auswertung von Reports eine Reduzierung der Administrationskosten für Sicherheitstools, sowie die Beseitigung der zuvor erwähnten Herausforderungen. Die Autoren [RK11] beschreiben SCAP als ein Mehrzweckprotokoll, welches automatisierte Verwundbarkeitsanalysen, technische Compliance- Kontrollaktivitäten und das Securitymeasurement über Herstellergrenzen hinweg unterstützt.

In Abbildung 7 nach [QSBJ11] sieht man zusammenfassend, aus welchen Komponenten sich das SCAP aufbaut. Die Gruppierung erfolgte nach

„Enumerations“, „Vulnerability Measurement and Scoring“ und „Expression and Checking Languages“.

Die Gruppe der „Enumerations“ beinhaltet Nomenklaturen, Nachschlagewerke für den Bereich Security und produktbezogene Informationen. Die „Vulnerability Measurement and Scoring“-Gruppe umfasst Spezifikationen für die Messung der Charakteristiken von Verwundbarkeiten, sowie die Erstellung von Bewertungen anhand dieser Charakteristiken. Die letzte Gruppe „Expression and Checking Languages“ setzt sich aus XML-Schemata zur Spezifizierung von Checklisten und zur Erzeugung von Checklisten Reports zusammen. Jede dieser SCAP-Komponenten hat somit einen bestimmten Zweck zu erfüllen und könnte unabhängig von den anderen genutzt werden. Von Seiten der Entwickler wird allerdings empfohlen, nicht auf einzelne Komponenten zu verzichten, denn nur so kann der Mehrnutzen des SCAP vollständig ausgeschöpft werden. [QSBJ11]

SCAP Component	Description	Maintaining Organization
Enumerations		
Common Configuration Enumeration (CCE)	Nomenclature and dictionary of system configuration issues	MITRE Corporation
Common Platform Enumeration (CPE)	Nomenclature and dictionary of product names and versions	MITRE Corporation
Common Vulnerabilities and Exposures (CVE)	Nomenclature and dictionary of security-related software flaws	MITRE Corporation
Vulnerability Measurement and Scoring		
Common Vulnerability Scoring System (CVSS)	Specification for measuring the relative severity of software flaw vulnerabilities	Forum of Incident Response and Security Teams (FIRST)
Expression and Checking Languages		
Extensible Configuration Checklist Description Format (XCCDF)	Language for specifying checklists and reporting checklist results	National Security Agency (NSA) and NIST
Open Vulnerability and Assessment Language (OVAL)	Language for specifying low-level testing procedures used by checklists	MITRE Corporation

Abbildung 7: SCAP Komponenten [QSBJ11]

Die Autoren [QSBJ11] des Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0 stellten in diesem Zusammenhang eine Sammlung von Empfehlungen zusammen, die Unternehmen einhalten sollten, um in den Genuss der Vorteile des SCAPs zu kommen. In Tabelle 3

sieht man eine Auflistung der Empfehlungen, nähere Details dazu sind aus [QSBJ11] zu entnehmen.

Auflistung der Empfehlungen:
• Organizations should use **security configuration checklists** that are expressed using SCAP to improve and monitor their systems' security.
• Organizations should take advantage of SCAP to **demonstrate compliance with high-level security requirements** that originate from **mandates, standards, and guidelines.**
• Organizations should use **standardized SCAP enumerations—identifiers and product names.**
• Organizations should use **SCAP for vulnerability measurement and scoring**.
• Organizations should acquire and use **SCAP-validated products**
• **Software developers** and **checklist producers** should **adopt SCAP** and use its capabilities.

Tabelle 3: Empfehlungen zur Einführung von SCAP nach [QSBJ11]

Der von NIST entwickelte Ansatz des SCAPs dürfte aus heutiger Sicht in näherer Zukunft enorm an Bedeutung gewinnen. Immer mehr renommierte Sicherheitsmanagementlösungsanbieter nutzen das Security Content Automation Protocol in ihren Produkten, um Software- und Konfigurations-Schwachstellen standardbasiert zu erkennen und direkt zu beseitigen. Eine vollständige Liste der SCAP zertifizierten Produktanbieter findet man unter http://nvd.nist.gov/scapproducts.cfm.

5 Herausforderungen für ein nachhaltiges IT-Security Managementkonzept

Das Themengebiet der IT-Security sieht sich ständig verändernden Herausforderungen gegenüber. Diese beginnen bei organisatorischen Umstrukturierungen innerhalb von Unternehmen und reichen bis hin zu neuen Bedrohungsszenarien und Angriffsmethoden über das Internet. Grundsätzlich stellt sich die Frage, was sich verändern kann und wo diese Veränderungen in Unternehmen auftreten können. Darauf gilt es, entsprechend zu reagieren und gegebenfalls die IT-Security anzupassen. In diesem Kapitel der Arbeit werden schrittweise aktuelle und zukünftige Herausforderungen an ein nachhaltiges IT-Security Managementkonzept für KMUs erfasst, aus denen sich im Folgekapitel Anforderungen für die Umsetzung eines solchen ableiten lassen.

In dem Dokument des „National Coordination Office for Networking and Information Technology Research and Development“ [NCO05] aus den USA wurden mehr als 30 Reports bezüglich der zukünftigen Herausforderungen an die IT-Security durchgeführt. Laut amerikanischen Sicherheitsexperten zählen diese zu den Hauptprioritäten, um die IT-Infrastrukturen weltweit zu schützen und sind somit auch für Unternehmen relevant.

In den anschließenden Kapiteln wird näher auf die Herausforderungen eingegangen, die es zukünftig für kleine und mittlere Unternehmen zu berücksichtigen gilt. Es handelt sich dabei um Herausforderungen allgemein an die IT-Security, aber auch um spezifische auf Unternehmen ausgerichtete. Speziell für kleine und mittlere Unternehmen ist es von Vorteil, diese Herausforderungen jetzt schon in ihre Sicherheitskonzepte einfließen zu lassen, um dadurch zukünftige Anpassungen zu vermeiden und Kosteneinsparungen zu erlangen.

5.1 Authentifizierungstechnologien

Authentifizierungstechnologien sind ein wesentlicher Bestandteil von vernetzten Einheiten wie Hardware, Software, Daten und Benutzer. Sie werden für eine Vielzahl von Verwendungszwecken benötigt, wie zum Beispiel Identifizierung, Autorisierung und Integritätsüberprüfung. Die Herausforderung besteht darin, dass diese Authentifizierungstechnologien zum einen sicher sein müssen, aber auch einfach verifizierbar sein sollten, eine Menge von Komponenten unterstützen und darüber hinaus schnell ausführbar sind. Die Autoren von [NCO05] sehen die Schwäche darin, dass man sich zwar auf spezielle Methoden in der Kryptographie bezüglich Security fokussiert hat, diese aber nicht effizient genug für die Authentifizierung von Millionen von Datenpaketen sind, beispielsweise durch einen einfachen Netzwerkrouter, welche in riesigen Netzwerken und Umgebungen wie dem Internet übertragen werden. [NCO05]

5.2 Protokollsicherheit

Ein weiteres heikles Thema ist die Sicherheit von Protokollen im Internet. Beispiel hierfür wäre die Weiterleitung von Datenverkehr auf eine alternative Seite eines Angreifers, um so Protokolle wie das Border Gateway Protocol (BGP) oder Dienste wie das Domain Name System (DNS) abzuhören.

Das BGP ist ein Routingprotokoll, das für die Kontrolle der Wege zuständig ist, die Datenpakete im Internet nehmen. Eine wesentliche Schwäche des BGP ist es, dass es keinerlei Methoden zur Authentisierung und Autorisierung von Kommunikationspartnern vorsieht. Ursprünglich wurde das BGP basierend darauf designt, dass es sich um vertrauenswürdige Teilnehmer handelt. Daher wurden auch keine Sicherheitsmaßnahmen umgesetzt. Darüber hinaus prüft das BGP nicht, ob ein Adressraum zu einem Autonomen System (AS) gehört oder nicht. Unter Autonomen Systemen versteht man eine gewisse Anzahl von IP-Netzen, die durch eine Organisation administriert und zu einer logischen Einheit zusammengefasst werden. [SC08], [KLS00]

Das DNS kontrolliert die Adressierung von Paketen. Es setzt sich aus zwei grundlegenden Mechanismen zusammen. Symbolische Hostnamen werden in IP-Adressen übersetzt, und vice versa. Bekannte Hauptprobleme hierbei sind, dass auf Informationen vertraut werden muss, die von nicht authentifizierten Quellen stammen; der namensbasierte Authentifizierungsprozess und dass zusätzliche Informationen übermittelt werden, welche gar nicht Bestandteil einer Anfrage waren oder inkorrekt sind. Dies führt dazu, dass Angreifer dadurch den Internetverkehr unterbrechen, überwachen oder auch verändern können und dies oftmals völlig unbemerkt. [LMMM00], [NCO05]

Demzufolge müssen Anstrengungen dahingehend unternommen werden, die Basisprotokolle besser zu schützen, um Gefahren wie Denial-of-Service-Attacken einzuschränken, die Beschädigung und Verfälschung von Informationen zu vermeiden und das Internet zu einem verlässlicheren Kommunikationsmedium zu machen. Zu diesem Themenbereich zählen unter anderem auch das Voice of Internet Protocol (VoIP), Web- und Virtual Private Network (VPN) Sicherheit. [NCO05]

5.3 Identitätsmanagement

Das Identitätsmanagement wird auch in Zukunft eine zentrale Rolle zum Schutz sensibler Daten eines Unternehmens darstellen. Verstärkt durch Trends wie Cloud Computing oder IT-Consumerization (näheres dazu im Kapitel 5.11) gilt als unerlässlich, dieses Themengebiet zu berücksichtigen.

Für Unternehmen stellt sich die Frage, wie sie gewährleisten können, Sicherheitsanforderungen hinsichtlich des rechtmäßigen Zugangs, der Vertraulichkeit der Daten, rechtlicher Aspekte sowie der Compliance zu erfüllen. Es stellt sich die Frage, wie man die klassischen Konzepte des Identitätsmanagements der Zugriffssteuerung und Kontrolle auf die neuen Technologien anwenden kann. Bisher wurden klassische Identitätsmanagement-Lösungen in Form eines ganzheitlichen Konstrukts über ein System eines Unternehmens gelegt. Der Abdeckungsgrad dieser Lösungen erstreckt sich normalerweise aber nur bis hin zur Unternehmensgrenze und

nicht darüber hinaus. Daraus lässt sich schlussfolgern, dass Unternehmensinfrastrukturen bzw. dessen Identitätsmanagement aus heutiger Sicht nicht für die Integration von Cloud Computing Services wie Infrastructure-as-a-Service oder Software-as-a-Service ausgelegt sind. Eine Lösungsmöglichkeit, um diesem Problem Herr zu werden, ist das Federal Identity Management. [CSA10], [SM09]

Ein weiterer Aspekt ist die kontinuierlich steigende Anzahl an User-Accounts für Mitarbeiter, Kunden, Partner, Lieferanten etc., bei denen eine Fülle von Passwörtern, Rollen und Berechtigungen administriert werden müssen. Die Unternehmen sind laufenden Veränderungen unterworfen, Abteilungsstrukturen verändern sich, Abteilungen werden neu geschaffen, werden zusammengelegt oder aufgelöst. Dadurch kommt es auch zu Anpassungen bezüglich der Rollen und Rechte der Mitarbeiter, die gemanagt werden müssen. Des Weiteren erfolgen Mitarbeiterwechsel in kürzeren Zyklen bzw. ändern sich ihre Rollen im Unternehmen immer häufiger. Dies hat für die IT-Security zur Konsequenz, dass ständig Anpassungen des Identitätsmanagements vorgenommen werden müssen, um etwaige Security-Löcher zu beheben und sensible Daten weiterhin adäquat zu schützen. [SM09]

Zusammenfassend lässt sich sagen, dass Identitätsmanagement als ein Basisbaustein für die IT-Security dient, um die Vermögenswerte zu schützen, Datenverlust und Diebstahl zu vermeiden und um gesetzliche Rahmenvorgaben zu erfüllen.

5.4 Sicheres Software Engineering und Softwaresicherheit

Ein wesentliches Problem für die einfache Verbreitung von Viren und Würmern stellt unsichere Software dar. Die heutigen Praktiken des Software Engineerings erlauben es, Programme zu implementieren und zu verbreiten, welche gefährliche Fehler beinhalten, zum Beispiel Pufferoverflows. Für Angreifer ist es dadurch einfach möglich, „Malicious Code“ in kritische Software einzufügen. Es gibt eine Menge an Herausforderungen, die es in diesem Bereich zu bewältigen heißt. Beispielsweise müssen Programmiersprachen und

Systeme grundlegende Sicherheitsfeatures beinhalten; der Code muss unabhängig von der Umgebung, in der er deployed wird, sicher bleiben; es muss Technologien geben, welche verifizieren und validieren, ob dokumentierte Sicherheitsanforderungen auch wirklich umgesetzt wurden. [NCO05]

5.5 Ganzheitliche Systemsicherheit

Eine effektive Sicherheit kann nur dann garantiert werden, wenn man nicht nur die einzelnen Komponenten eines Systems oder einer Infrastruktur in Betracht zieht. Die bereits zuvor erwähnten Herausforderungen, wie die Bereitstellung von wirksamen Authentifizierungstechnologien, sicheren Protokollen für grundlegende Operationen im Web und auch verbessertes Software Engineering Softwaresicherheit wirken in den Ansatz der ganzheitlichen Systemsicherheit ein. Es müssen sowohl Hardware, Betriebssysteme, Netzwerke, Applikationen und Mitarbeiter einbezogen werden, um eine ganzheitliche Systemsicherheit zu ermöglichen. [NCO05]

5.6 Monitoring und Nachweis von Angriffen

Auch wenn die Herausforderungen an ein nachhaltiges IT-Security Management berücksichtigt und bewältigt werden, wird man voraussichtlich nicht hundertprozentige Sicherheit garantieren können. Es ist damit zu rechnen, dass auch in Zukunft unerwartete Sicherheitsprobleme auftreten werden, auf die es zu reagieren gilt. Gegenwärtige Monitoringtools, welche irreguläre Netzwerkaktivitäten aufzeichnen, sind laut der Autoren [NCO05] bei weitem noch nicht ausgereift. Ziel ist die Schaffung von dynamischen Schutzmechanismen, welche sofort entsprechend reagieren, wenn Angriffe nachgewiesen wurden. Weiters besteht die Herausforderung darin, Monitoring so umzusetzen, dass es beispielsweise den Sicherheitsrichtlinien eines Unternehmens entspricht.

5.7 Datensicherheit - Verfügbarkeit von Systemen und Daten

Der Fokus in der IT-Security bewegt sich bei vielen Unternehmen weg vom Schutz vor externen Bedrohungen durch Firewalls, Antivirus etc., hin zu einem

verstärkten Schutz der Daten selbst. Da Firmendaten oftmals zu den wichtigsten und sensibelsten Assets zählen, umfassen die Schutzmaßnahmen nicht nur die Verschlüsselung dieser, sondern es wird vermehrt auch nach verstärkten Zugriffs- und Nutzungskontrollmechanismen verlangt. Die Herausforderung besteht darin, integrierte IT-Sicherheitslösungen anzubieten, die den Datenschutz im erweiterten Kontext zum Datenmanagement enthalten. [BBZBJ10] Im Zuge einer ausreichenden Datensicherheit muss die IT-Security auch dafür gewappnet sein, um auf unvorhersehbare Angriffe möglichst schnell reagieren zu können, damit die Verfügbarkeit von Systemen und Daten sichergestellt ist.

5.8 Unabhängigkeit von der technologischen Ebene

Eine weitere Herausforderung an die IT-Security ist der Umgang mit den verschiedenen Technologien. Unternehmen stützen sich oftmals auf eine Vielzahl von verschiedenen Technologien. Die Herausforderung für die IT-Security liegt darin, dass sie fähig sein muss, neue Hard- und Software integrieren zu können. Dies schon allein, um ein gewisses Maß an Interoperabilität zu gewährleisten. Diverse Hardware und auch Software besitzen unterschiedliche Anforderungen an die IT-Security. Es muss berücksichtigt werden, dass beispielsweise Software auf verschiedenen Betriebssystemen läuft, sei es Windows, Unix, Mac OS, Android usw. All diese Betriebssysteme besitzen Stärken und Schwächen, die nicht vernachlässigt werden dürfen. Die Herausforderung für eine nachhaltige IT-Security ist, unabhängig von der dahinterliegenden Technologie, Systeme und Software so zu integrieren, dass auch deren Verwundbarkeiten bezüglich der Security beachtet und minimiert werden. [NCO05]

5.9 Veränderung des Geschäftsfeldes und Geschäftsmodells

Im Normfall ist die Geschäftstätigkeit eines Unternehmens, auf der die Existenz aufbaut, klar definiert und die IT-Security darauf abgestimmt. Jedoch können die Struktur und die Anzahl der Geschäftsfelder je nach Größe des Unternehmens variieren. Dies hat zur Folge, dass die IT-Security auf die

einzelnen Bereiche abgestimmt sein sollte. Oftmals haben einzelne Geschäftsfelder eine höhere Priorität an Schutzbedarf als andere. Dies kann verschiedene Gründe haben; Kernprozesse, die wesentlich zum Unternehmenserfolg beitragen und dadurch nicht ausfallen dürfen, haben sicherlich eine höhere Priorität bezüglich des Schutzes als Supportprozesse. Geschäftsfelder, in denen die Datensicherheit von enormer Bedeutung ist, sollten ebenfalls überwiegend im Fokus der IT-Security stehen.

Im Rahmen von wirtschaftlichen Gründen könnte es beispielsweise durch Marktsättigung, Konzentration auf einen neuen Wachstumsmarkt oder die Einführung von neuen Technologien dazu kommen, dass sich Unternehmen gezwungen bzw. veranlasst sehen, ihr Geschäftsfeld/ Modell zu verändern. Dadurch ergeben sich neue Herausforderungen für IT-Security Verantwortliche, mit denen sie umzugehen wissen sollten. Eine Auflistung dieser könnte wie folgt aussehen:

- **Priorität des Schutzbedarfs von Prozessen ändert sich:** neu geschaffene oder veränderte Prozesse rücken in den Fokus, um die Geschäftsziele zu erfüllen. Ältere Prozesse sind dann möglicherweise weniger oder gar nicht mehr relevant.
- **Abhängigkeiten zwischen Prozessen ändern sich:** in modernen Unternehmensgefügen gibt es eine Vielzahl von Abhängigkeiten, zum einen zwischen Prozessen untereinander, zum anderen auch zur Informationstechnologie.
- **Sicherheitsrechtliche Aspekte (Datensicherheit, Datenschutz) ändern sich:** im Rahmen der Veränderung des Geschäftsfelds/ Modells kann es auch dazu kommen, dass sicherheitsrechtliche Aspekte einbezogen werden müssen, die zuvor für das Unternehmen nicht relevant waren oder nun angepasst werden sollten.
- **Ausfallszeiten für Prozesse/Produkte ändern sich:** Durch Veränderungen des Geschäftsfelds/ Modells muss sich ein Unternehmen der Herausforderung stellen, dass die Ausfallszeiten für Prozesse und

Produkte angepasst werden müssen; geänderte Ausfallszeiten gehen vielerorts auch mit Veränderungen der dahinterliegenden IT-Security Architektur einher. Hierbei spielt der Faktor der Verfügbarkeit von Prozessen eine wichtige Rolle.

- **Neue Technologien kommen zum Einsatz:** der Einsatz neuer Technologien kann nur einen Teil des Unternehmens betreffen, sich aber auch über Unternehmensgrenzen hinweg bemerkbar machen. Es entstehen neue Anforderungen an die IT-Infrastruktur, welche mit einbezogen werden müssen.
- **Organisationsstruktur muss angepasst werden:** Die Änderung des Geschäftsfelds/ Modells verursacht in den meisten Fällen die Notwendigkeit zur Anpassung der Organisationsstruktur. Beispielsweise werden Abteilungen ausgelagert, neue Abteilungen geschaffen und Mitarbeiter eingestellt oder versetzt. All dies bedarf Überlegungen, die in ein nachhaltiges IT-Security Managementkonzept einfließen müssen. Siehe dazu Kapitel 5.10.
- **Bedrohungsszenarien ändern sich:** die Änderung des Geschäftsfelds/ Modells führt dazu, dass parallel zu diesem Vorgang neue Risiken und Gefahrenquellen für das Unternehmen wirksam werden.
- **Neue Absatzwege entstehen:** die Änderung des Geschäftsfelds/ Modells könnte auch eine Änderung der Absatzwege mit sich bringen. Bei vielen Firmen gibt es die Tendenz, traditionelle Absatzwege an die neuen Anforderungen wie E-Business und E-Commerce anzupassen. Diese Umstrukturierungen und das zusätzliche Involvieren von Informationstechnologie stellt Unternehmen ebenfalls vor neue Herausforderungen.

Je nach Branche oder Auslegung des Geschäftsmodells eines Unternehmens variieren die Herausforderungen. Finanzdienstleister haben

üblicherweise andere Prioritäten bezüglich IT-Security, als beispielsweise ein Herstellerunternehmen.

5.10 Veränderung der Organisationsstruktur

Der ständige Wettbewerb in einer globalisierten Welt verlangt von Unternehmen, ständig Anpassungen auch an der Organisationsstruktur vorzunehmen, um weiterhin wettbewerbsfähig und rentabel zu sein. Wie bereits im vorhergehenden Kapitel erwähnt, können Änderungen des Geschäftsfelds bzw. des Modells zur Anpassung der Organisationsstruktur führen. Unternehmensübernahmen, Fusionen oder auch der in den letzten Jahren immer mehr an Bedeutung gewinnende Begriff des „Outsourcing“ führen dazu, dass die Organisationsstrukturen laufend angepasst werden müssen. In diesem Rahmen gibt es eine Vielzahl von Herausforderungen, die es zu bewältigen gilt. Nachstehend eine Auflistung dieser:

- **Mergen (Zusammenführen) der IT-Infrastruktur:** Das „Mergen“ der IT-Infrastruktur stellt eine wichtige Herausforderung dar, sei es bei einer Unternehmensübernahme oder einer Zusammenlegung von Abteilungen oder Standorten eines Betriebs. Verschiedene Unternehmen bzw. Abteilungen setzen auf unterschiedliche Hardware-Technologien, Sicherheitsstandards- und Konzepte, Softwarepakete usw.
- **Gefahrenquellen ändern sich:** Natürlich führt die Veränderung der Organisationsstruktur auch zum Auftreten neuer Risiken und Bedrohungen.
- **Aspekt des Mitarbeiters:** In den meisten Fällen sind auch Mitarbeiter von Änderungen der Organisationsstruktur betroffen. Mitarbeiter, die in unterschiedlichen Unternehmen bzw. Abteilungen tätig waren, haben anderes Vorwissen bezüglich IT-Sicherheit. Dieses Vorwissen gilt es anzugleichen. Mitarbeiter müssen beispielsweise hinsichtlich Sicherheitsrichtlinien und im Umgang mit sensiblen Unternehmensdaten geschult werden.

- **Outsourcing:** Das „Outsourcen“ (Auslagern) von Abteilungen bis hin zu ganzen Sparten gewinnt in den letzten Jahren immer mehr an Einfluss. Grundsätzlich unterscheidet man zwischen internem und externem Outsourcing. Von internem Outsourcing spricht man, wenn beispielsweise eine Auslagerung eines Teils eines Konzerns in ein eigenes Unternehmen stattfindet. Bei externem Outsourcing werden Unternehmensaufgaben an Drittunternehmen bzw. Fremdfirmen ausgelagert. Outsourcing findet oftmals dann statt, wenn kostenintensive Aufgaben abgetreten werden sollen, um Kapazitäten im Unternehmen freizumachen oder es kompetente Dienstleister dafür gibt.

  Durch das Outsourcen werden zum einen zwar Risiken und komplexe Bereiche eines Unternehmens ausgelagert, für die dann der Drittunternehmer haftet. Zum anderen werden sensible Informationen und Daten in die Hände von Dritten gegeben, was bezüglich der Sicherheit auch ein Risiko darstellen kann. Aus diversen Umfragen geht hervor, dass viele Unternehmen weder einen genauen Überblick über die externen Zugriffsrechte haben, noch ausreichend überprüft wurde, ob der Dienstleister auch die relevanten Datenschutzanforderungen erfüllt. [BBZBJ10] Die Herausforderung hierbei besteht darin, die Vor- und Nachteile abzuwägen und sich beispielsweise mittels Service-Level-Agreements (SLAs) abzusichern.

5.11 Veränderung durch externe Bedrohungsszenarien & neue Technologien

Die Veränderung der Bedrohungsszenarien stellt eine der größten Herausforderungen an ein funktionierendes nachhaltiges IT-Security Managementkonzept dar. Wie bereits in den vorhergehenden Kapiteln erwähnt, bringen jegliche Umgestaltungen in Unternehmen, seien es Veränderungen des Geschäftsfelds/ Modells oder der Organisationsstruktur neue Bedrohungsszenarien mit sich, welche sich nur schwer vermeiden lassen. Durch den Einsatz neuer Technologien, Einstellung neuer Mitarbeiter bzw.

Zuteilung zu anderen Aufgabengebieten rücken unterschiedliche Prozesse in den Fokus der IT-Security und sicherheitsrelevante Aspekte müssen an die neuen Gegebenheiten angepasst werden. Jedoch führen nicht nur angestrebte und gelenkte Veränderungen innerhalb der Unternehmen zum Auftauchen neuer Bedrohungsszenarien. Die von außerhalb gesteuerte Technologieweiterentwicklung, sowie neue Trends in der IT wie beispielsweise IT-Consumerization, Unified Communications, Cloud-Computing führen für Unternehmen dazu, sich neuen Herausforderungen zu stellen.

Sogenannte Internet-Bedrohungen, die häufig auch als Malware zusammengefasst werden, zählen zur Kategorie der externen Bedrohungsszenarien und sind nach wie vor eine wesentliche Bedrohung für die IT-Security. Dieser Typus von Schadprogrammen zeichnet sich durch ausgeklügelte Methoden und Techniken aus, die sich über Netzwerke wie das Internet weiterverbreiten. Darüber hinaus entwickeln sie sich ständig weiter und werden in ihren Funktionsweisen an neue entdeckte Schwachstellen angepasst. Ein Hauptproblem bei Angriffen aus dem Internet mittels Malware ist, dass eine zunehmende Professionalisierung bzw. Industrialisierung beim Vorgehen und Durchführen dieser externen Angriffe stattfindet.

Angriffe werden vermehrt gezielt geplant und zentral gesteuert. Neue Sicherheitslücken, sei es in Soft- oder Hardware, werden sehr schnell ausgenutzt. Man spricht dabei auch von sogenannten „Zero Day Exploits“. Die Angreifer bauen zwischenmenschliche Beziehungen (Stichwort: „Social Engineering“) auf, um Angriffsziele vorher auszukundschaften. Ein weiterer Trend ist, dass diese Angriffe vermehrt aus kommerziellen Interessen heraus erfolgen. Angriffe gegenüber Unternehmen und auf deren Systeme werden als Dienstleistung gegen Entgelt angeboten. Nicht nur beim Vorgehen und der Durchführung von Angriffen kommt es zu einer immer rapideren Weiterentwicklung, sondern auch bei den eingesetzten Schadprogrammen bzw. Malware und Werkzeugen. Sie zeichnen sich durch immer kürzere Entwicklungszyklen aus, sind modular aufgebaut und können sich beispielsweise selbst über integrierte Update-Funktionen aktualisieren. Ein

weiterer Grund für das enorme Bedrohungspotential von Malware liegt darin, dass sie mittlerweile schon „on-demand“ im Internet erzeugt werden können, selbst von Personen ohne Fachkenntnisse. [BBZBJ10]

In einem nachhaltigen Security Managementkonzept müssen auch diese Faktoren berücksichtigt werden. Nur wenn man bedenkt, dass sich die Bedrohungsszenarien ständig ändern und sich die Technologie laufend weiterentwickelt, kann man sich nachhaltig auf zukünftige Ereignisse vorbereiten.

Die bereits zuvor erwähnten Trends in der IT wurden deshalb hervorgehoben, weil sie laut einer Vielzahl an Expertenartikeln als eine der größten Herausforderungen für die kommenden Jahre angesehen werden. In den anschließenden Unterkapiteln wird kurz ihre zunehmende Bedeutung für die IT-Security hervorgehoben.

5.11.1 IT-Consumerization

IT-Consumerization ist einer der aufstrebenden Trends der letzten Monate. Darunter ist zu verstehen, dass Mitarbeiter bzw. Endanwender von IT-Produkten ihre eigens privat angeschafften IT-Endgeräte an den Arbeitsplatz mitbringen und diese beruflich auch nutzen. Häufig handelt es sich dabei um Smartphones, Tablet PCs, Netbooks usw. Diese sogenannten „Consumer technologies“ bringen einen großen Nutzen und eine steigende Mobilität der Anwender mit sich. Arbeiten können von Zuhause oder unterwegs effizient abgewickelt werden. Der Zugriff auf das Firmennetzwerk ist von überall möglich, Emails können jederzeit abgerufen werden, man ist sozusagen ständig up-to-date, was zu einer steigenden Produktivität führen kann. [BOU10]

Hingegen ergeben sich durch diesen Trend auch neue Risiken für die IT-Security, die es zu managen gilt. Die IT-Consumerization führt dazu, dass Unternehmen die Kontrolle über die zu schützenden Endgeräte verlieren. Zum einen verfügen nicht alle Endgeräte über entsprechende Sicherheitseigenschaften (die sie haben sollten), zum anderen können jene Endgeräte, die nicht im Besitz des Unternehmens sind, bezüglich Security nicht

ausreichend überprüft und gemanagt werden. Des Weiteren verschwimmen durch die IT-Consumerization zusätzlich die Grenzen, ob ein Endgerät sich nun innerhalb des Firmennetzwerks befindet oder auch nicht, von welchem Typ es ist, welche Sicherheitsvorkehrungen es besitzt oder welcher Kategorie von User es zugeteilt ist. Die zentrale Herausforderung ist es, trotz des Einzugs der „consumer technolgies“ in die Unternehmen, die Datensicherheit zu gewährleisten. Es ist wichtig zu wissen, wie man sich zukünftig effektiv davor schützt, dass Daten in die Hände von Dritten gelangen, durch die Nutzung von PDAs, Smartphones etc. keine neuen Angriffspunkte auf das Firmennetzwerk geöffnet werden und in Folge dadurch auch keine Malware eingeschleust wird. [BOU10]

5.11.2 Unified Communications

Ein weiterer Trend der IT ist der Übergang zu Unified Communications (UC) in Unternehmen. Durch die Integration von Kommunikationsmedien in dafür vorgesehene Anwendungsumgebungen wird eine vereinheitlichte Kommunikation angestrebt. Ziel ist es, moderne Telekommunikationsmedien und IT-Anwendungen ineinander verschmelzen zu lassen. Kommunikationskanäle wie Telefon, Fax, Email, PDAs, Instant Messaging oder Conferencing werden unter einer Benutzeroberfläche gebündelt und in die IT-Anwendungen eines Unternehmens eingebunden. UC sollte nicht als einzelnes Produkt angesehen werden, sondern als ein Konglomerat der verschiedenen Komponenten. Eine Voice-over-IP (VoIP) Infrastruktur bietet in den meisten Fällen die Basis für UC-Lösungen. Das heißt, Daten und Sprache werden über ein gemeinsames IP-basiertes Netz geleitet [Ber10].

Durch den Einsatz von UC bietet sich für Unternehmen die Möglichkeit, ihre Unternehmenskommunikation effizienter und einfacher zu machen. Darüber hinaus lassen sich dadurch die Kosten reduzieren und es ergeben sich neue Potentiale durch die verbesserte Kommunikation im Unternehmen. UC führt in den meisten Fällen zur Produktivitätssteigerung, sowohl für den einzelnen Mitarbeiter, Arbeitsgruppen als auch für das ganze Unternehmen.

Allerdings bringt die Einführung einer neuen Technologie und deren Mehrnutzen, wie in den meisten solcher Fälle auch zusätzliche Risiken und Verwundbarkeiten mit sich, die es zu bewältigen gilt. Wie bereits zuvor erwähnt, sind die heutigen Unified Communications Lösungen IP-basiert, woraus sich ableiten lässt, dass die Firmenkommunikation mehrheitlich über das Internet abläuft. Schlagwörter bezüglich der Sicherheitsrisiken, die sich durch die Einführung von IP-basierten UC-Lösungen ergeben, sind VoIP-Sniffing, DoS-Attacken auf die Kommunikationsinfrastruktur, Ausspähen von Instant Messages und anderem Datenverkehr, die Beeinträchtigung der Verfügbarkeit und die Veränderung von Daten, Verbreitung von Viren, etc. [AL11]. Da eine UC-Lösung ein Konglomerat von vielen verschiedenen Komponenten ist, besitzt sie auch eine Vielzahl von Angriffspunkten, die geschützt werden müssen. Eine unsichere UC-Lösung führt zur Verletzung der primären Schutzziele und kann darüber hinaus enormen Schaden für das Unternehmen verursachen, wenn man bedenkt, welche Auswirkungen der Eintritt der oben genannten Sicherheitsrisiken haben könnte.

Da UC aber aufgrund seiner vielen Vorteile in Zukunft immer häufiger in Unternehmen umgesetzt werden wird, sollte in einem nachhaltigen IT-Security Managementkonzept dieser Aspekt und dessen Herausforderungen an die IT-Security auf alle Fälle hinzugezogen werden.

5.11.3 Cloud Computing

Mittels des gegenwärtigen Trends des Cloud Computing haben Anwender die Möglichkeit, auf dynamische, skalierbare und verteilte Anwendungen über ein Netzwerk zuzugreifen. Dies sollte aber unter den Bedingungen erfolgen, dass die drei wesentlichen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt sind. Die Nutzung der Technologie des Cloud Computings bietet Unternehmen die Möglichkeit, ihre Investitionskosten und ihre Betriebskosten zu reduzieren. Des Weiteren erlaubt Cloud Computing Unternehmen, effizient und schnell auf einen Pool von Ressourcen zuzugreifen.

Dies führt jedoch zu einer Aufweichung der Außengrenzen von Unternehmensnetzen und Anwendungen. Dadurch fällt es sehr schwer, sie mit einem undurchdringlichen Schutz aus Firewalls, Intrusion Detection Systems (IDS), Content Filtering und Data-Loss-Prevention-Systemen zu versehen [BBZBJ10].

Die heutigen Herausforderungen im Cloud Computing sind weitreichend und umfassen Punkte wie die Datensicherheit, den Standort der Storage-Datencenter, Fehlen von Service-Level-Agreements (SLAs), Verletzung von Compliance-Anforderungen, sowie die Kontrolle und Klassifizierung der Daten in der Cloud. Weiters sollte bedacht werden, dass Cloud-Infrastrukturen auch für etwaige Hardwaredefekte oder einen simplen Stromausfall anfällig sein können. [Kau09]

Üblicherweise ist ein Unternehmen für den Schutz von personenbezogenen Daten vor Missbrauch, Verlust, unautorisiertem Zugriff, Veränderung und Offenlegung verantwortlich. Werden nun Daten in die Cloud ausgelagert, führt dies wiederum dazu, dass sich Unternehmen darum kümmern müssen, dass der Cloud Service Provider die entsprechenden Sicherheitsmaßnahmen zur Verfügung stellt, um die Daten eines Unternehmens entsprechend zu schützen. Fehlen nun entsprechende SLAs mit dem Service Provider kann die Datensicherheit nicht in dem Ausmaß gewährleistet werden, wie sie beispielsweise in der Sicherheitsrichtlinie des Unternehmens festgelegt wurde oder gesetzlich vorgegeben ist. Befindet sich nun der Cloud Service Provider in einem anderen Land oder auf einem anderen Kontinent, kommen erschwerend einige Faktoren hinzu, die es zu beachten gilt. Befindet sich das Storage-Datencenter eines Cloud Service Providers beispielsweise in Indien und garantiert dieser, dass er die Datensicherheit gewährleistet, muss dies aber nicht zwingend bedeuten, dass dem auch tatsächlich so ist. Zurück zu führen ist dies darauf, dass Datensicherheitsgesetze, sowie Privacy-Gesetze von Land zu Land unterschiedlich sein können. Der Cloud Service Provider garantiert zwar für die Datensicherheit, jedoch unter anderen gesetzlichen Vorgaben, die nicht denen des Kunden entsprechen müssen. [OVPC11]

Wie man sieht gibt es allein bezüglich der Datensicherheit einige Herausforderungen im Bereich des Cloud Computings zu bewältigen. Dabei sind Bedenken, was passieren könnte, wenn der Service Provider in Konkurs geht oder wie die Daten nach Ablaufen eines Vertrags zerstört werden, noch gar nicht berücksichtigt.

5.11.4 Virtualisierung

Virtualisierung wird sich in den nächsten Jahren zunehmend zu einer Standardtechnologie für Unternehmen entwickeln. Mittels Virtualisierung können beispielsweise auf einem PC oder Server simultan verschiedene Betriebssysteme oder auch mehrere Sessions eines Betriebssystems ausgeführt werden. Dadurch können nun eine Vielzahl von Applikationen und Funktionen auf einem einzigen Gerät ausgeführt werden, anstatt wie früher, wo man dafür mehrere separate Maschinen benötigte.

Die Herausforderung liegt heute darin, diese virtualisierten Systeme auch adäquat zu schützen, da sie genau so anfällig für Bedrohungen sind wie physische Systeme. Es gibt jedoch Unterschiede, denn viele virtualisierte Systeme laufen auf derselben Maschine, benötigen aber einen unterschiedlichen Level an Schutz. Dies hat zur Folge, dass man die Security nicht wie bisher auf die komplette Maschine auslegen kann, sondern differenziert vorgehen muss. Viele Unternehmen gehen von dem Ansatz aus, dass eine virtualisierte Maschine genauso zu schützen ist wie ein normales Betriebssystem und passen ihre existierenden Guidelines, Standards und Tools dementsprechend an. Experten sehen auch eine Gefahr in dem Trend, virtuelle Maschinen im Rahmen eines Austausches oder Upgrades eines physischen Servers von einem Gerät auf ein anderes zu verlegen, ohne zu bedenken, dass dieses vielleicht gar nicht im Stande ist, die virtuelle Maschine zu schützen. [VAU08]

Ein weiteres Gefahrenpotential liegt darin, dass virtuelle Netzwerkverbindungen nicht immer durch die physischen Netzwerksverbindungsschutzmaßnahmen abgedeckt sind. Die Basisschutzmechanismen für Netzwerksicherheit decken

normalerweise nicht die Kommunikation zwischen den virtuellen Maschinen auf einem Server ab. Dieser fehlende Einblick auf den Verkehr zwischen den virtualisierten Maschinen bietet die Möglichkeit, unentdeckte Angriffe durchzuführen, deren Auswirkungen anschließend das ganze physische System beeinflussen können. [VAU08]

Das größte Gefahrenpotential bei der Virtualisierung stellt der „Hypervisor“ oder auch „Virtual Machine Monitor“ dar. Es handelt sich dabei um eine Software, die eine Umgebung für virtuelle Maschinen schafft. Er verteilt die bereitstehenden real verfügbaren Ressourcen eines Rechners an die virtuellen Maschinen. Die Funktionalität des Hypervisors ermöglicht ihm somit auch, dass er Zugriff auf die Hardwareressourcen hat, teilweise auch uneingeschränkten Zugriff. Erlangt man durch einen Angriff die Kontrolle über den Hypervisor, liegen das dahinterliegende System, sowie die darauf virtualisierten Maschinen offen für den Eindringling. [VAU08]

Zusammenfassend lässt sich sagen, dass die oben erwähnten Herausforderungen an die Security im Bereich der Virtualisierung in Zukunft einen kritischen Faktor für Unternehmen darstellen und somit in einem nachhaltigen Security Managementkonzept definitiv berücksichtigt werden sollten.

6 Anforderungen an ein nachhaltiges IT-Security Managementkonzept

Die Anforderungen an ein nachhaltiges IT-Security Managementkonzept für kleine und mittlere Unternehmen sind genau so vielfältig wie die Herausforderungen. Sie ergeben sich aus allgemeinen Anforderungen bezüglich IT-Security die es zu erfüllen gilt und individuellen, die sich aus den Herausforderungen aus Kapitel 5 ableiten lassen. In den folgenden Kapiteln werden wesentliche Anforderungen schrittweise analysiert und beschrieben. Die Einordnung der Anforderungen erfolgt in Anlehnung an die ITIL Best Practices auf allen Management-Ebenen [BSI05] und dem Security-Paradigma des British Standard 7799 [BÖ05].

In Abbildung 8: IT-Security Pyramide ist die IT-Security Pyramide dargestellt, welche sich über alle Managementebenen eines Unternehmens erstreckt. Jede dieser Ebenen bezieht sich auf verschiedene Bereiche der IT-Security.

Auf strategischer Ebene wird die IT-Security Politik festgelegt. [BÖ05] Die Etablierung und Initiierung der IT-Security im Unternehmen erfolgt mittlerweile auf strategischer Ebene, durch die Managementorgane. Sie definieren den Stellenwert der IT-Security und geben die IT-Strategie für das Unternehmen vor – im Gegensatz zu früher, als die IT-Security als eine technische Disziplin angesehen war und die IT-Mitarbeiter als Initiatoren galten, da meistens nur sie das Wissen, die Fähigkeiten und die Ressourcen im Umgang mit Sicherheitsfragen hatten. [CA04]

Die taktische Ebene umfasst konkrete Vorgaben und Vorgehensweisen an die IT-Security. Dieser Bereich beschäftigt sich vorwiegend mit der Fragestellung, was zu tun ist, um eine adäquate Sicherheit in Unternehmen garantieren zu können. Beispiele hierfür wären die Festlegung einer Sicherheitsrichtlinie, eines konkreten Sicherheitskonzepts, Aufbau einer Sicherheitsarchitektur und auch die Einbeziehung von existierenden Planungsansätzen.

Die operative Ebene beschäftigt sich mit den konkreten Maßnahmen der IT-Security. Das heißt hier kommen Tools und Werkzeuge zum Einsatz, um Security Konzepte umzusetzen und die IT-Security Politik des Unternehmens zu leben. Im Rahmen dieser Arbeit werden auch die konkreten Anforderungen an die operative Ebene zur Einführung eines nachhaltigen IT-Security Managementkonzepts beschrieben. Dazu zählen beispielsweise die Kommunikation der Sicherheitsrichtlinie, Mitarbeiterschulungen und Awarenesstrainings oder auch der Einsatz von sicherer Software etc.

Die in dieser Arbeit angewandte IT-Security Pyramide beruht auf dem Konzept, dass die jeweils höhere Ebene den Rahmen und die Vorgaben für die tiefer liegende Ebene vorgibt. Des Weiteren nehmen die Granularität, sowie die Technikorientierung bezüglich der einzusetzenden Maßnahmen sukzessive zu, während die organisatorischen Aspekte in den Hintergrund rücken [BÖ05].

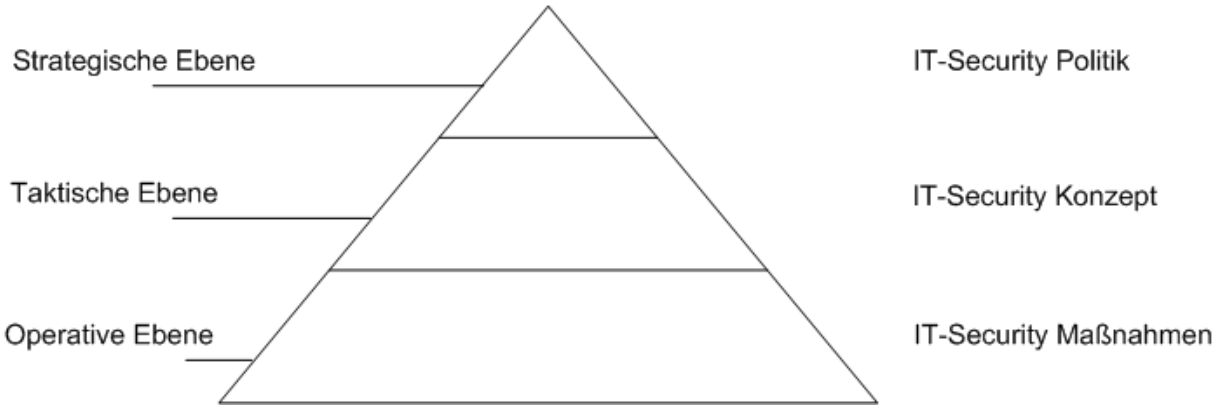


Abbildung 8: IT-Security Pyramide [eigene Darstellung]

Zu beachten ist in jedem Fall, dass eine Vielzahl der anschließend beschriebenen Anforderungen somit nicht als gesondert betrachtet werden können, da sie aufeinander aufbauen und es zwischen ihnen Abhängigkeiten und Wechselwirkungen gibt, sowohl auf derselben Ebene als auch

übergreifend. Anhand der beschriebenen IT-Security Pyramide werden in den folgenden Kapiteln die Anforderungen an ein nachhaltiges IT-Security Managementkonzept, die ihnen entsprechenden Ebenen zugeordnet und erläutert.

6.1 Anforderungen an die strategische Ebene

Der Anstoß zur Einführung eines nachhaltigen IT-Security Managementkonzepts muss von der Führungsebene initiiert werden. Es handelt sich hierbei um die strategische Ausrichtung des Bereichs Security im Unternehmen. Die Bedeutung von Security muss von oben kommuniziert und positioniert werden.

Dazu sollten von der Führungsebene jene wesentlichen Anforderungen berücksichtigt werden, die in den nachfolgenden Kapiteln beschrieben sind.

6.1.1 Nachhaltigkeit, Wartbarkeit und Skalierbarkeit

Eine der grundlegenden Anforderungen an ein funktionierendes IT-Security Managementkonzept ist es, die Prämissen der **Nachhaltigkeit, Wartbarkeit** und **Skalierbarkeit**, die bereits in Kapitel 2 erläutert wurden, in der IT-Security Strategie zu verankern. Durch die Einhaltung der Nachhaltigkeit wird sichergestellt, dass ein entworfenes IT-Security Managementkonzept nicht nur den heutigen Anforderungen der IT-Security entspricht, sondern auch auf zukünftige Veränderungen ausgelegt ist. Deshalb ist es auch unerlässlich, beispielsweise neue Technologien in den Anforderungskatalog einzubeziehen und zukünftige, möglicherweise aufstrebende und eintretende Bedrohungsszenarien so gut wie möglich zu berücksichtigen. Die Wartbarkeit steht in einem engen Zusammenhang zur Nachhaltigkeit. Um die Anforderungen der Nachhaltigkeit zu erfüllen, muss das entworfene Security Managementkonzept entsprechend wartbar sein. Gerade im Bereich der Security kommt es laufend zum Auftreten neuer Herausforderungen und Anforderungen. Durch die Wartbarkeit und die Skalierbarkeit kann garantiert werden, dass diese laufend in ein bestehendes Security Managementkonzept eingearbeitet bzw. berücksichtigt werden.

6.1.2 Einhaltung der Schutzziele zum Schutz der Unternehmenswerte

Als ein integraler Bestandteil jedes Security Managementkonzepts müssen die Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit erfüllt werden. Zur Umsetzung der Schutzziele gibt es eine Vielzahl an Maßnahmen. Entsprechend der individuellen Anforderungen des Unternehmens müssen diese abgewogen und ausgewählt werden, denn nicht immer muss eine durchgeführte Maßnahme effektiv und zielführend sein. Prinzipiell lässt sich aber festhalten, dass nur durch Einhaltung und Erfüllung der Schutzziele die wesentlichen Assets eines Unternehmens geschützt werden. Es macht keinen Sinn, weitere Schutzmaßnahmen zu ergreifen, wenn nicht die primären Schutzbedürfnisse zufriedenstellend erfüllt wurden. Für Sicherheitsverantwortliche von Firmen ist es wichtig, ein gutes Verständnis über die essentiellen Unternehmenswerte zu besitzen und wo deren Verwundbarkeiten liegen. Da die Einhaltung der Schutzziele von enormer Bedeutung für alles Sicherheitsaspekte ist, werden sie der strategischen Ebene zugeordnet und müssen von der Managementebene als wesentlicher Bestandteil im Managementkonzept verankert werden.

6.1.3 Einführung einer durchgehenden Sicherheitsstrategie

Ein weiterer Bestandteil für ein nachhaltiges IT-Security Management ist die Etablierung einer durchgehenden Sicherheitsstrategie für Unternehmen, um eine ganzheitliche Systemsicherheit zu schaffen. Auf strategischer Ebene erfolgt die Festlegung der Eckpfeiler für die Sicherheitsstrategie, die es auf den unteren Ebenen (taktisch und operativ) umzusetzen gilt. Zu diesen zählen auch die bereits erwähnten Prämissen der Nachhaltigkeit, Wartbarkeit, Skalierbarkeit und auch die Einhaltung der Schutzziele zum Schutz der Unternehmenswerte. Die Schaffung eines Sicherheitsprozesses und der Bedarf nach einer Informationsrichtlinie oder eines Sicherheitskonzepts an sich im Unternehmen sind klassische Faktoren, die in eine Sicherheitsstrategie einfließen sollten. In den meisten Fällen wird ein angestrebtes Sicherheitsniveau für das Unternehmen in der Strategie festgelegt und dazu ein Maßnahmenpaket zur Erreichung dieser Ziele geschnürt. Dementsprechend müssen von der

Managementebene finanzielle, personelle und zeitliche Ressourcen zur Verfügung gestellt werden, um die entworfene Sicherheitsstrategie anschließend auch adäquat umsetzen zu können [BSI09].

6.2 Anforderungen an die taktische Ebene

Im Allgemeinen bezieht sich die taktische Ebene auf die Erfüllung der Zielvorgaben und Vorgehensweisen zur Erreichung der Security-Ziele der strategischen Ebene. In den folgenden Kapiteln werden exakt jene Anforderungen an die taktische Ebene zur Umsetzung eines nachhaltigen IT-Security Managementkonzepts beschrieben.

6.2.1 Minimierung der klassischen Risikofaktoren

Die Vermeidung eines Sicherheitsbruchs durch Minimierung der klassischen Risikofaktoren ist eine weitere wesentliche Anforderung, die es zu beachten gilt. Dieser tritt dann ein, wenn die Risikofaktoren aus Kapitel 3.1 schlagend werden. Wie bereits erwähnt, hätte ein Sicherheitsbruch zur Folge, dass es zu einer Offenlegung, Verweigerung, Zerstörung oder Veränderung von Systemen kommen kann, beziehungsweise deren Daten.

Die Wahrscheinlichkeit des Eintritts eines Sicherheitsbruchs kann minimiert werden, wenn die klassischen Risikofaktoren berücksichtigt werden. Das heißt, es müssen neben den Unternehmenswerten die verschiedenen Gefahrenquellen, seien es zufällig auftretende, umweltbedingte oder beabsichtigte und die Verwundbarkeiten, sowie deren Ausprägungen mit einbezogen und vermieden werden. Nachstehend in Tabelle 4 werden zusammenfassend nochmals die Typen von Gefahrenquellen und Verwundbarkeiten aufgelistet.

Gefahrenquellen	Verwundbarkeiten bezüglich der
Physische Gefahrenquellen	Infrastruktur
Bezüglich der technischen Ausstattung	Hardware
Menschliche Gefahrenquellen	Software
Höhere Gewalt	Kommunikation
	Mitarbeiter

Tabelle 4: Ausprägungen von Gefahrenquellen und Verwundbarkeiten [eigene Darstellung]

Als ein effizientes Mittel zur Minimierung der klassischen Risikofaktoren sollten **Risikoanalysen** durchgeführt werden. Im Rahmen einer Risikoanalyse können mögliche Verwundbarkeiten und deren potentieller Schaden aufgedeckt werden. Nach Charles P. Pfleeger [PFL00] können Risikoanalysen folgenden positiven Nutzen für Unternehmen haben:

- Identifikation von weiteren kritischen Unternehmens-Assets und Verwundbarkeiten
- Rechtfertigung für getätigten oder noch zu tätigenden Sicherheitsaufwand
- Verbesserung der Awareness im Unternehmen
- Eine Basis für zukünftige Security-Entscheidungen

Sicherheitsverantwortliche sollten sich den entsprechenden Gegenmaßnahmen zur Beseitigung bzw. Reduzierung der Gefahrenquellen und Verwundbarkeiten bewusst sein. Dazu können technische Maßnahmen, physische Maßnahmen wie auch taktische Maßnahmen zählen.

6.2.2 Einführung bzw. Umsetzung einer Sicherheitsrichtlinie (Policy)

Ein Schlüsselelement jedes IT-Security Managementkonzepts ist eine effektive und gut konzipierte Sicherheitsrichtlinie in elektronischer, aber speziell auch in dokumentierter Form. Das heißt, es ist wichtig, alle Überlegungen bezüglich der Sicherheit schriftlich festzuhalten, denn nur dann ist sie analysierbar, nachvollziehbar und nachweisbar [KK08]. Sie deckt die relevanten Aspekte zur Sicherstellung der Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit ab und kann daher als ein Grundsatzdokument für Unternehmen angesehen werden.

Nach den Autoren Heinrich Kersten, Gerhard Klett [KK08] und dem deutschen Bundesamt für Sicherheit in der Informationstechnik [BSI] sollte eine effektive Sicherheitsrichtlinie zumindest folgende Punkte umfassen:

- **Kurze Beschreibung des Unternehmens:** Charakterisierung des Geschäftszwecks, grobe Abbildung der Organisationsstruktur und gegebenenfalls eine Aufzählung der Standorte
- **Beschreibung der Sicherheitsziele und der Sicherheitsstrategie:** Welche konkreten Sicherheitsziele verfolgt das Unternehmen? Was sind die Kernelemente der Sicherheitsstrategie?
- **Beschreibung des Stellenwerts der IT-Sicherheit:** welchen Wert besitzt die IT-Sicherheit für das gesamte Unternehmen bzw. einen bestimmten Anwendungsbereich? Welche Auswirkungen können etwaige Sicherheitsvorfälle haben?
- **Festlegung des Geltungsbereichs der Sicherheitsleitlinie:** für welchen Bereich bzw. welche Geschäftsprozesse des Unternehmens ist sie gültig?
- **Vorgaben zur Einhaltung der Sicherheit:** gesetzliche oder vertragliche Bestimmungen.
- **Hinweise zu Schulungs- und Sensibilisierungsmaßnahmen**

Darüber hinaus ist das ständige Begutachten und eventuelle Verbessern der Sicherheitsleitlinie von großer Bedeutung, um zu prüfen, ob getätigte Aussagen in der Leitlinie noch aktuell sind. So ändern sich beispielsweise Geschäftsprozesse sowie die unterstützendende Technik laufend. Bei der Erstellung einer Sicherheitsrichtlinie ist zu beachten, dass die Sicherheitsverantwortlichen ein näheres Verständnis bezüglich der Geschäftsanforderungen des Unternehmens benötigen. Nur dann kann eine zweckdienliche Sicherheitsrichtlinie entworfen bzw. umgesetzt werden.

Je nach Bedarf empfiehlt das [BSI], unterschiedliche Sicherheitsrichtlinien und Teilkonzepte zu erstellen, die die einzelnen IT-Sicherheitsthemen bedarfsgerecht darstellen. Dadurch erhalten Mitarbeiter eines Unternehmens genau jene Informationen, die sie zu einem bestimmten Thema benötigen. In Anbetracht dessen, dass Sicherheitsrichtlinien maximal zehn Seiten umfassen sollten, könnte eine Aufteilung nach Sicherheitsthemen ebenfalls angedacht werden.

6.2.3 Einführung einer (IT-)Compliance/ Abdeckung sicherheitsrechtlicher Aspekte

Eine weitere Anforderung an ein nachhaltiges IT-Security Managementkonzept ist die Integration eines (IT-)Compliance Prozesses in den Unternehmen. Compliance beschreibt im Allgemeinen jene Aktivitäten, die ein regelkonformes Verhalten herbeiführen, unter Bereitstellung entsprechender Hilfsmittel zur Abbildung der Unternehmenslage. Mittels der Einführung eines Compliance-Prozesses kann zum einen die Gesetzeskonformität (gesetzliche Vorgaben) gewährleistet werden, zum anderen kann überprüft werden, ob unternehmensinterne festgelegte regulative Vorgaben (Richtlinien, Normen, Standards, Best-Practices) eingehalten werden [TA09].

Die IT-Compliance fokussiert sich im Wesentlichen auf die Aspekte von Compliance Anforderungen, welche die IT-Systeme eines Unternehmens betreffen. Dazu zählen üblicherweise die Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz. Ein weiterer Grund ist die stetig

wachsende Anzahl an Standards, Normen, Gesetzen und Prüfungen, die es auch im Bereich der IT zu beachten gilt.

Im Papier [TA09] werden zwei Herangehensweisen für Organisationen zur Einführung einer IT-Compliance vorgestellt. Es müssen jene Regulierungen identifiziert werden, welche es verpflichtend zu befolgen gilt und Frameworks oder Praktiken, denen gegenüber sie konform sein sollten (siehe Tabelle 5).

	Verpflichtende Einhaltung von…	**(Teilweise verpflichtend) Im Einklang/ konform mit …**
	Gesetzen, Regeln und Regulierungen	Standards, Frameworks, Security Praktiken
Beispiele	Datenschutzrichtlinien, EU-Richtlinien, Basel II, Sarbanes Oxley Act (SOX), EUROSoX, etc.	ISO 2700x, IT-Grundschutzkatalog, Common Criteria, COBIT, ISO 9000 etc.

Tabelle 5: Beispiele zur Einführung einer IT-Compliance [eigene Darstellung]

Daraus lässt sich schlussfolgern, dass das Einführen eines IT-Compliance Prozesses zu einer dauerhaften Einhaltung von formulierten Compliance-Anforderungen führt, was in weiterer Folge natürlich positive Auswirkungen auf die IT-Sicherheit mit sich bringt.

6.2.4 Berücksichtigung existierender Planungsansätze der IT-Security

Wie bereits in Kapitel 4 erwähnt, gibt es existierende Planungsansätze, die sich auf verschiedene Bereiche der IT-Security auswirken. Jeder für sich bietet Vorteile und Nachteile hinsichtlich Umsetzung und geht von einem etwas anderen Blickwinkel an das Themengebiet der IT-Security heran. Die ISO 2700x Reihe beispielsweise könnte man als vollständiges Vorgehenskonzept zur Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems ansehen.

Der BSI Grundschutzkatalog wird vielerorts als eine detaillierte Informationsbasis zur Schaffung einer gewissen Basissicherheit für IT-Objekte (Anwendungen, IT-Systeme, Räumlichkeiten Netze) angesehen, obwohl auch er eigentlich einem bestimmten Vorgehenskonzept zum Aufbau einer Sicherheitsorganisation entspricht. Das österreichische Sicherheitshandbuch grenzt sich durch eine kompaktere Darstellungsweise ab, die speziell mittleren und kleineren Unternehmen entgegen kommen soll. Weiters wurde in dieser Arbeit zusätzlich der Common Criteria (CC) Ansatz vorgestellt, der zur Bewertung der Sicherheit von Informationstechnologie in Unternehmen dient.

Selbstverständlich gibt es noch andere Planungsansätze, die sich im entfernteren Zusammenhang mit der IT-Security beschäftigen. Hierzu seien als Schlagwörter CobiT (Control Objectives for Information and Related Technology) ein international anerkanntes Framework zur IT-Governance erwähnt oder die ITIL (IT Infrastructure Library), die als eine Sammlung von Best-Practices zur Umsetzung eines IT-Service Managements beschrieben werden kann.

Als Anforderung für die Umsetzung eines nachhaltigen IT-Security Managementkonzepts sollten je nach den Bedürfnissen des Unternehmens existierende Planungsansätze bzw. Teile dieser berücksichtigt werden, vorausgesetzt man ist sich bewusst, welche es gibt und wie diese bestmöglich auf das Unternehmen umzulegen sind. Das hätte den Vorteil, dass ein gewisser Standard an Sicherheit für Unternehmen gewährleistet ist. Bereits erwähnte Anforderungen wie die Einhaltung der Schutzziele zum Schutz der Unternehmenswerte oder die Minimierung der klassischen Risikofaktoren wären dadurch ebenso abgedeckt.

Lässt man sich dann noch bezüglich einem dieser international anerkannten Standards zertifizieren, wissen auch externe Partner und Kunden, dass IT-Security im Unternehmen einen gewissen Stellenwert inne hat. Als positiver Nebeneffekt einer Zertifizierung könnten ebenfalls vorgegebene Compliance-Anforderungen erfüllt werden.

6.2.5 Berücksichtigung der Schwachstellen bezüglich der Protokollsicherheit

Um die Nachhaltigkeit eines IT-Security Managementkonzepts sicherzustellen, ist es notwendig, die in Kapitel 5.2 aufgezeigten Schwachstellen bezüglich der Protokollsicherheit im Internet zu berücksichtigen. Wie bereits erwähnt, besitzen das Border Gateway Protocol (BGP) oder das Domain Name System (DNS) in ihrer jetzigen Form gravierende Mängel in Bezug auf sicherheitsrelevante Aspekte wie Authentisierung, Autorisierung und Authentifizierung, was beispielsweise zu Denial-of-Service-Attacken und zur Beschädigung und Verfälschung von Informationen/Daten führen kann. Zukünftige Entwicklungen zur Verbesserung des Internets als verlässliches Kommunikationsmedium müssen hier einbezogen werden. Darüber hinaus sollte in Betracht gezogen werden, dass etwaige Sicherheitsvorfälle auf die Schwächen in der Protokollsicherheit zurückzuführen sind. Konkret sollte ein Augenmerk auf die Weiterentwicklung des S-BGP(Secure Border Gateway Protocol) gelegt werden, sowie auf zusätzliche Security-Funktionen wie TSIG (Transaction Signatures) und DNSSEC (DNS-Security), um die DNS Sicherheit zu garantieren.

6.2.6 Auslegung auf Prozesse und deren Veränderungen

Um den Ansatz des prozessorientiertem Denkens, der der de-facto Standard in Unternehmen ist, erfüllen zu können, müssen Überlegungen getätigt werden, wie die IT-Security direkt an die Prozesse gekoppelt werden kann. Früher gab es technikorientierte Ansätze in Hinblick auf die IT-Security. Der Einfachheit halber wurden für potentiell gefährdete Prozesse entsprechende technische Sicherheitsmaßnahmen durchgeführt, ohne sich näher Gedanken über die Verflechtungen von etwaigen Sicherheitsanforderungen zu machen.

Erfahrungen zeigen jedoch, dass es im Laufe der letzten Jahre eine Wandlung hin zum **sicherheitsorientierten Prozessdesign** als praktikableren Ansatz gab. Die IT-Security muss von Beginn an, sei es in der Entwicklung von Prozessen, wie auch bei deren Anpassungen, einbezogen werden. Das

Durchführen von **Schutzbedarfsanalysen** für die einzelnen Prozesse eines Unternehmens stellt eine wichtige Anforderung an ein nachhaltiges IT-Security Managementkonzept dar. Dabei gilt es, die essentiellen Kernprozesse zu definieren, die grundsätzlich einen höheren Schutzbedarf benötigen. Dies können Prozesse sein, die einen enormen Einfluss für die unternehmerische Wertschöpfung besitzen, als auch Prozesse, in denen sensible Informationen (z.B Mitarbeiter- oder Kundendaten) benötigt bzw. verarbeitet werden.

Kommt es zur Veränderungen bzw. Anpassungen von Prozessen oder der Organisationsstruktur im Unternehmen, beeinflusst dies auch die IT-Security. Die Anforderung besteht darin, möglichst schnell zu erkennen, wo nun genau Sicherheitsmaßnahmen zu treffen sind und ob durch die Veränderungen auch andere Prozesse und Organisationseinheiten betroffen sind.

Eine weitere Anforderung an die Auslegung eines nachhaltigen IT-Security Managementkonzepts auf Prozesse ist, dass man auf die sich ständig ändernden Bedrohungsszenarien entsprechend reagieren können muss. Das heißt, das zum Einsatz kommende Sicherheitsmanagementkonzept sollte so entworfen sein, dass auf das Auftreten einer neuen Bedrohung entsprechend reagiert werden kann. Es sollte nachvollziehbar zu überprüfen sein, für welchen Prozess das Auftreten eines neuen Bedrohungsszenarios eventuell Konsequenzen haben könnte. Näheres zu den Bedrohungsszenarien im Kapitel 6.2.10.

Im Rahmen eines sicherheitsorientierten Prozessdesigns sollten zusätzlich Überlegungen bezüglich Outsourcings durchgeführt werden. Es gilt abzuwägen, ob es sinnvoll ist, Einzelleistungen, Teilprozesse oder gar vollständige Geschäfts- oder Managementprozesse in die Hände externer Dienstleister zu geben. Dies kann dann der Fall sein, wenn das eigene Unternehmen nicht das geforderte Sicherheitsniveau garantieren kann, oder dies nur durch großen Einsatz finanzieller Mittel möglich wäre. Entschließt man sich für das Outsourcing eines Bereichs des Unternehmens, sollte überprüft werden, inwieweit der Dienstleister für die notwendige Security garantiert und ob auch

relevante Datenschutzanforderungen erfüllt sind. Darüber hinaus ist es eine unerlässliche Anforderung, Service-Level Agreements zu vereinbaren, in denen die zu erbringende Leistung festgehalten wird, damit Unternehmen sich selbst absichern können, falls es zu Sicherheitszwischenfällen seitens des Dienstleisters kommt.

6.2.7 Berücksichtigung neuer Technologien

Die Berücksichtigung neuer Technologien stellt ebenso eine wesentliche Anforderung dar, um die Nachhaltigkeit des Managementkonzepts sicherzustellen. Die Eingliederung neuer Technologien bzw. die Anpassung der IT-Infrastrukturen an diese, stellt Unternehmen ständig vor neue Herausforderungen hinsichtlich der IT-Security, wie bereits im Kapitel 5.11 erwähnt. Man muss sich nur die aktuellen Entwicklungen hinsichtlich Unified Communications, den Trend hin zur IT-Consumerization, Cloud Computing und Virtualisierung in Erinnerung rufen, die zahlreiche Fragestellungen bezüglich der IT-Security aufwerfen. Selbstverständlich kann der Einsatz neuer Technologien aber auch einen zusätzlichen Nutzen für Unternehmen bringen, der sich in weiterer Folge möglicherweise als ein Wettbewerbsvorteil herausstellt.

Ein weiterer nicht unerheblicher Faktor ist der Zeitpunkt der Einführung einer neuen Technologie. Ein frühes Zurückgreifen auf eine neue Entwicklung kann zur Folge haben, dass diese noch nicht ausgereift ist und somit einen enormen Risikofaktor für das Unternehmen darstellt. Wartet man hingegen zu lange, könnte die Technologie zwar hinsichtlich diverser Sicherheitsrisiken hinreichend ausgereift sein, jedoch möglicherweise nicht mehr up-to-date und den Anforderungen des Unternehmens entsprechend.

Es ist daher notwendig für ein nachhaltiges IT-Security Managementkonzept, die Einführung neuer Technologien in Unternehmen zu berücksichtigen und diese bestmöglich zu integrieren, ohne dass das bestehende Sicherheitsniveau vermindert wird.

6.2.8 Unabhängigkeit des Security Managementkonzepts von der technologischen Ebene

Ein weiteres wesentliches Merkmal der heutigen Zeit ist, dass es laufend und in immer kürzeren Zyklen zu Innovationen und Weiterentwicklungen in der Branche der IT-Technologien kommt. Wie bereits im Kapitel 6.2.7 erwähnt, müssen neue Technologien berücksichtigt werden, schon deshalb, um die Nachhaltigkeit des Security Managementkonzepts sicherzustellen und ein gewisses Maß an Interoperabilität zu gewährleisten.

Das zu entwerfende Security Managementkonzept muss darüber hinaus unabhängig von bereits bestehenden Technologien sein, sei es auf Hardware oder auch auf Softwareebene. Es muss die Fähigkeit besitzen, diverse Technologien integrieren zu können, mit dem Ziel, auftretende Verwundbarkeiten, beispielsweise durch unterschiedliche Sicherheitsanforderungen oder Inkompatibilität minimieren zu können.

6.2.9 Fähigkeit, auf Umstrukturierungen der IT reagieren zu können

Das „Mergen“ bzw. Zusammenführen von IT-Infrastrukturen stellt häufig eine Herausforderung dar, sei es bei Unternehmensübernahmen, Zusammenlegungen von Abteilungen oder Standorten eines Betriebs. Unterschiedliche Unternehmen und Abteilungen setzen oftmals auf unterschiedliche Hardware-Technologien, Sicherheitsstandards- und Konzepte, Softwarepakete usw. Im Zuge von Umstrukturierungen sind in vielen Fällen auch Anpassungen der IT-Infrastruktur notwendig. Es ist eine wesentliche Anforderung, entsprechende Maßnahmen im Security Managementkonzept vorzusehen, die einen reibungslosen Ablauf bei Umstrukturierungen in der IT garantieren, ohne dass das bestehende Sicherheitsniveau eines Unternehmens darunter leidet, oder es sogar zum Auftreten von neuen Verwundbarkeiten kommt.

6.2.10 Berücksichtigung neuer Bedrohungsszenarien

Eine wichtige Anforderung ist es, sowohl bestehende als auch neue Bedrohungsszenarien, soweit dies möglich ist, hinsichtlich der IT-Security zu

berücksichtigen. Wie bereits im Kapitel der Herausforderungen erwähnt, gibt es vielseitige Gründe, die zur Entstehung neuer Bedrohungsszenarien führen. Aus diesem Anlass werden nochmals die wesentlichen Gründe aufgezählt, die zum Auftreten dieser führen können:

- Umstrukturierungen im Unternehmen (Veränderungen des Geschäftsfelds/ Modells, Anpassung der Organisationsstruktur, Einführung neuer Prozesse, Anpassung bestehender Prozesse)
- Der stetig steigende Einfluss der IT auf private und betriebliche Abläufe
- Einsatz neuer Technologien bzw. Technologieweiterentwicklung
- Einstellung neuer Mitarbeiter
- Schwachstellen der bestehenden IT-Infrastruktur
- Internet-Bedrohungen
- Soziale Netzwerke
- Zunehmende Professionalisierung von Angriffen

Nur durch die Berücksichtigung dieser vielseitigen Gründe für das Auftreten neuer Bedrohungsszenarien können präventive Maßnahmen ergriffen werden, um die IT-Infrastrukturen ausreichend zu schützen.

6.3 Anforderungen an die operative Ebene

Nicht nur auf strategischer und taktischer Ebene gibt es Anforderungen zur Umsetzung eines nachhaltigen IT-Security Managements. In den nachfolgenden Kapiteln werden verpflichtende Anforderungen an die operative Ebene erhoben.

6.3.1 Kommunikation der Sicherheitsrichtlinie

Das Bestehen einer allgemeinen Sicherheitsrichtlinie bzw. spezifischer Dokumente mit unterschiedlichen Inhalten in einem Unternehmen garantiert noch lange nicht, dass dies auch von den Angestellten gelebt wird. Eine wesentliche Anforderung auf operativer Ebene ist, neben der Einführung von

Sicherheitsrichtlinien die Kommunikation dieser an die Mitarbeiter. Dafür gilt es entsprechend der Zielgruppen die Formulierungen so anzupassen, dass die Mitarbeiter die Sicherheitsrichtlinien auch verstehen können. Es ist nicht zielführend, wenn die eingesetzten Formulierungen unverständliche Fremdwörter enthalten oder sich zu sehr in Details verstricken.

Ein weiterer nicht unerheblicher Faktor bei der Kommunikation an die Mitarbeiter ist es, ihnen klar zu machen, dass eine Nichteinhaltung der Sicherheitsrichtlinie Konsequenzen nach sich zieht. Abgesehen davon, dass durch ein Nichtbeachten ein enormer betriebswirtschaftlicher Schaden verursacht werden kann und oftmals wesentliche Sicherheitsaspekte verletzt werden. Die Mitarbeiter sind davon zu unterrichten, dass eine Nichteinhaltung der Sicherheitsrichtlinie für denjenigen Mitarbeiter, der diese missachtet, Sanktionen zur Folge hat. Nur so kann garantiert werden, dass sich auch wirklich jeder verantwortungsvoll mit dem Thema auseinander setzt.

6.3.2 Mitarbeiterschulungen bzw. Awarenesstrainings

Mitarbeiterschulungen und/oder Awarenesstrainings sind eine weitere Anforderung an ein Unternehmen auf operativer Ebene, um die Mitarbeiter bezüglich der Bedeutung von IT-Sicherheit zu sensibilisieren. Ein adäquates Sicherheitsniveau auf hohem Level kann aber nur dann erreicht werden, wenn neben den vielen technischen und physischen Maßnahmen, die getroffen werden können, alle Mitarbeiter aktiv zur Sicherheit beitragen. Wie bereits zu Beginn der Arbeit erwähnt, stellt der Faktor Mensch einen wesentlichen Unsicherheitsfaktor hinsichtlich Sicherheit dar. Das Einführen bester technischer und zugleich teurer Schutzmaßnahmen nützt nichts, wenn diese durch persönliche Nachlässigkeit und Bequemlichkeit der Mitarbeiter ausgesetzt werden.

Daher ist es von enormer Bedeutung, den Angestellten die korrekte Handhabung der IT beizubringen und ihr Bewusstsein im Umgang mit dieser zu stärken, um eine hohe Sicherheit gewährleisten zu können. Wesentlich ist dabei, Interesse für das Thema Sicherheit bei den Mitarbeitern zu wecken und

ihnen grundlegende Fachkenntnisse zu vermitteln, damit diese Probleme an ihrem Arbeitsplatz auch selbst erkennen oder beheben können. Durch regelmäßige Schulungen, Workshops oder Newsletter kann das Interesse am Thema Sicherheit dauerhaft aufrecht erhalten werden. Ein Unternehmen kann dadurch enorme Investitionskosten in zusätzliche Sicherheitsmaßnahmen sparen, wenn das Risiko des Faktors Mensch minimiert wurde.

6.3.3 Bedarf nach einer fortlaufenden Auditierung

Der Bedarf nach einer fortlaufenden Auditierung dient Unternehmen zur Überprüfung, ob die Ziele, Vorgaben und Maßnahmen bezüglich der IT-Sicherheit entsprechend erfüllt werden. Mittels regelmäßig durchgeführten Sicherheitsaudits kann eine Vielzahl der bereits in dieser Arbeit definierten Anforderungen an die IT-Security auf ihre Wirksamkeit in Unternehmen geprüft werden. Beispielsweise kann überprüft werden, ob die Vorschriften der IT-Compliance erfüllt sind, ob bestehende Maßnahmen zur Aufrechterhaltung des Sicherheitsniveaus nach wie vor geeignet sind, ob diese korrekt umgesetzt und auch von allen Beteiligten eingehalten werden.

Weiterer Nutzen liegt darin, dass eventuelle Verwundbarkeiten und Sicherheitslücken der IT-Infrastruktur aufgedeckt werden können, ob und wo Anpassungen bei den Geschäftsprozessen und den zugehörigen Sicherheitsvorkehrungen zu treffen sind und ob zusätzliche Schulungs- und Awarenesstrainings für die Mitarbeiter notwendig sind.

6.3.4 Nutzung von effizienten Authentifizierungstechnologien

Verschlüsselung und Authentifizierung dienen als Basis, um Vertrauen zu schaffen und bilden die Grundlage für sichere Netzwerke, in denen Benutzer und Geräte zuverlässig identifiziert werden können. Authentifizierungstechnologien sind ein wesentlicher Bestandteil von vernetzten Einheiten wie Hardware, Software, Daten und Benutzer.

Schon allein daraus ergibt sich die Anforderung, dass bereits vorhandene Authentifizierungstechnologien, wie auch eventuelle Weiterentwicklungen

selbiger, in einem nachhaltigen Security Managementkonzept berücksichtigt werden müssen. Mittlerweile gibt es eine Vielzahl von Herangehensweisen und Technologieentwicklungen um die Authentifizierung zu gewährleisten, sei es auf Hardware- und Softwareebene (z.B. diverse Verschlüsselungsverfahren, Protokolle, Zertifikate, etc.) oder Benutzerebene (Passwörter, Smartcards, Biometrielösungen, etc.). Es muss individuell abgewogen werden, welche Verfahren zur Authentifizierung eingesetzt werden müssen und ob diese eventuell kombinierbar sind.

Zusammenfassend lässt sich sagen, dass der Einsatz effizienter Authentifizierungstechnologien für alle vernetzten Einheiten eine wesentliche Anforderung darstellt. Darüber hinaus sollten sie einfach verifizierbar sein, eine Vielzahl von Komponenten unterstützen und wenn möglich auch noch schnell ausführbar sein. Um das Potential der Authentifizierungstechnologien auszuschöpfen, sollten offene Standards zum Einsatz kommen, die für alle Anwendungen eingesetzt werden können. Sie sollten auf vorhandenen Anwendungs- und Netzwerkinfrastrukturkomponenten aufbauen, ohne dass zusätzliche Hardware oder Software erforderlich ist. Das heißt, es sollten etablierte Protokolle genutzt werden.

6.3.5 Umsetzung eines funktionierenden und nachhaltigen Identitätsmanagement

Wie bereits im Kapitel der Herausforderungen erwähnt, wird das Identitätsmanagement in Zukunft eine zentrale Rolle beim Schutz sensibler Daten in Unternehmen spielen und einen wichtigen Bestandteil einer funktionierenden IT-Security bilden. Eine wesentliche Anforderung an ein nachhaltiges Identitätsmanagement in Zukunft ist, dass es nicht nur innerhalb eines Unternehmens greift, sondern auch über die Unternehmensgrenzen hinweg. Zu den Auslösern dafür zählen die verstärkt auftretende globale Zusammenarbeit von Unternehmen und neue Trends in der Technologieentwicklung wie beispielsweise Cloud-Computing. Zudem stellen zusätzliche gesetzliche Anforderungen (Compliance), Schutz der

Unternehmenswerte und das ständige Auftauchen neuer Bedrohungsszenarien einen wesentlichen Faktor dar, der die Umsetzung eines nachhaltigen Identitätsmanagements verlangt. Eine Auslegung auf eine große Useranzahl, sowie eine einfache Administrierbarkeit und Pflege sind weitere Anforderungen, die sich aus den Herausforderungen aus dem Kapitel 5.3 ergeben.

Des Weiteren ist es unbedingt notwendig, die noch reifende und an Bedeutung gewinnende Technologie des Federal Identity Managements zu berücksichtigen. Ziel des Federal Identity Managements ist es, exakt jene zuvor beschriebenen Anforderungen, die sich mit dem Austausch von Identitätsdaten über die Unternehmensgrenzen hinweg beschäftigen, umzusetzen. Es soll eine organisationsübergreifende Übermittlung von personenbezogenen Daten zwischen Unternehmen ermöglicht werden.

6.3.6 Einsatz von sicherer Software

Der Einsatz von sicherer Software auf operativer Ebene sollte eigentlich ein elementarer Bestandteil in jedem Unternehmen sein. Speziell in einem nachhaltigen Security Managementkonzept darf diese Anforderung auf keinen Fall fehlen. Durch Berücksichtigung dieses Aspekts können schon im Voraus eine Vielzahl von Verwundbarkeiten für ein Unternehmen minimiert bzw. vermieden werden. Nähere Details bezüglich Gefahrenpotentiale von unsicherer Software sind nochmals im Kapitel 5.4 der Herausforderungen nachzulesen. Es sollten nur jene Softwaretechnologien zum Einsatz kommen, die grundlegende Sicherheitsfeatures beinhalten. Kritische Software, welche Fehler und Lücken aufweist oder noch nicht ausgereift ist, sollte auf keinen Fall im Regelbetrieb eines Unternehmens verwendet werden.

6.3.7 Einführung von Monitoringmechanismen

Die Notwendigkeit von Monitoringmechanismen gilt als eine zusätzliche Anforderung, die das zu entwerfende Security Managementkonzept umfassen muss. Schon allein deswegen, weil eine vollständige Sicherheit von IT-Infrastrukturen wie bereits einige Male in dieser Arbeit angemerkt wurde, niemals garantiert werden kann. Moderne Unternehmensgeflechte besitzen IT-

Infrastrukturen, die sich aus einer Vielzahl von Systemen zusammensetzen, die diverse Services anbieten und auf denen eine Menge an unterschiedlichen Applikationen laufen. Viele dieser Bestandteile einer IT-Infrastruktur sind für Angriffe von außen anfällig und weisen Verwundbarkeiten auf, die oftmals schwer einzudämmen sind. Deshalb ist es unerlässlich, sich mit der eventuellen Einführung von Monitoringmechanismen zum Schutz der Unternehmenswerte bzw. um irreguläre Netzwerkaktivitäten und in weiterer Folge getätigte Angriffe auf die IT Infrastruktur nachzuweisen zu können, einzuführen. Es gilt auch, die Weiterentwicklung der derzeitigen Monitoringtools zu beobachten, da hier zukünftig ein Augenmerk auf die Schaffung von dynamischen Schutzmechanismen gelegt wird, welche sofort und automatisch auf Angriffe reagieren, sobald diese nachgewiesen werden.

Eine weitere Anforderung von Monitoringtools ist es, dass sie bei Bedarf zur Überprüfung, ob festgelegte Sicherheitsrichtlinien erfolgreich im Unternehmen umgesetzt wurden, herangezogen werden können.

6.3.8 Bedarf nach Disaster Recovery und Datenwiederherstellung

Der Bedarf nach Disaster Recovery (Notfallwiederherstellung) und in weiterer Folge Datenwiederherstellung ist eine wesentliche Anforderung für ein nachhaltiges Security Management auf operativer Ebene. Wenn es trotz aller getroffenen Maßnahmen zu einem Sicherheitszwischenfall in einem Unternehmen kommen sollte, muss die Möglichkeit bestehen, die IT möglichst schnell, wenn auch nur eingeschränkt wieder zum Laufen zu bringen. Dadurch kann vermieden werden, dass es in Unternehmen zu einem Stillstand der Produktivität kommt. Dieser entsteht dadurch, dass mittlerweile nahezu alle Geschäftsabläufe von der IT abhängig sind.

Im Rahmen dessen gilt es auch den Begriff Business Continuity (Geschäftsfortbestand) zu berücksichtigen und umzusetzen. Diese garantiert, dass kritische und wichtige Geschäftsfunktionen für Unternehmen, auch bei Eintreten eines Sicherheitszwischenfalls weiterhin zur Verfügung stehen. Dafür ist es notwendig, jene Prozesse zu kennen, die für den Fortbestand der

Geschäftstätigkeiten unbedingt aufrechtzuerhalten sind und welche Maßnahmen dafür getätigt werden müssen.

Zusätzlich gibt es, wie bereits im Kapitel 6.2.6 beschrieben, auf taktischer Ebene die Anforderung, die IT-Security auf die Prozesse und deren Veränderungen auszulegen. Hierbei sollten auch diejenigen Prozesse eines Unternehmens identifiziert werden, welche einen erhöhten Schutzbedarf benötigen und welche Maßnahmen dafür erforderlich sind. Das heißt, wenn diese Anforderung ausreichend erfüllt ist, kann in weiterer Folge die Business Continuity leichter umgesetzt werden.

7 Entwurf eines nachhaltigen IT-Security Managementkonzepts

In diesem Kapitel wird das entworfene nachhaltige IT-Security Managementkonzept, sowie der dazugehörige Prozess zur Einführung desselbigen vorgestellt. Das Konzept hat den Zweck, die Unternehmen längerfristig und nachhaltig für den Umgang mit der IT-Security und den sich ständig verändernden Herausforderungen vorzubereiten. Durch die Umsetzung des entworfenen IT-Security Managementkonzepts, beispielsweise von IT-Security Verantwortlichen, soll ein Konzept etabliert werden, welches zum einen existierende grundlegende Anforderungen hinsichtlich der IT-Security berücksichtigt und zum anderen zukünftige Herausforderungen mit einbezieht.

Speziell kleinen und mittleren Unternehmen soll es als Grundlage dienen, die wichtigsten Anforderungen an die Security in ihrem Sicherheitskonzept zu erfassen. Offensichtlich ist, dass sich je nach Größe und Ausrichtung des Unternehmens die Anforderungen unterscheiden werden. Für ein mittleres Unternehmen mit einer größeren Anzahl an Mitarbeitern und einer komplexeren IT-Infrastruktur haben Faktoren wie die Einführung einer Sicherheitsrichtline, einer IT-Compliance oder Mitarbeiterschulungen und Awarenesstrainings höchstwahrscheinlich eine andere Bedeutung, als für einen kleinen Betrieb mit wenigen Mitarbeitern. Andererseits ist es für jedes Unternehmen, egal welcher Größe, wichtig, die klassischen Risikofaktoren zu minimieren, neue Technologien und Bedrohungsszenarien zu berücksichtigen und sichere Software einzusetzen.

Das entworfene IT-Security Managementkonzept soll genau diesen Aspekt berücksichtigen und somit jetzigen und zukünftigen Security-Anforderungen für kleine, als auch für mittlere Unternehmen gerecht werden.

Bevor das Security Managementkonzept vorgestellt wird, gilt es die wesentlichen Einflussfaktoren und Abhängigkeiten zwischen den bereits erwähnten Anforderungen und Risikofaktoren zu erfassen und in eine Beziehung zu stellen.

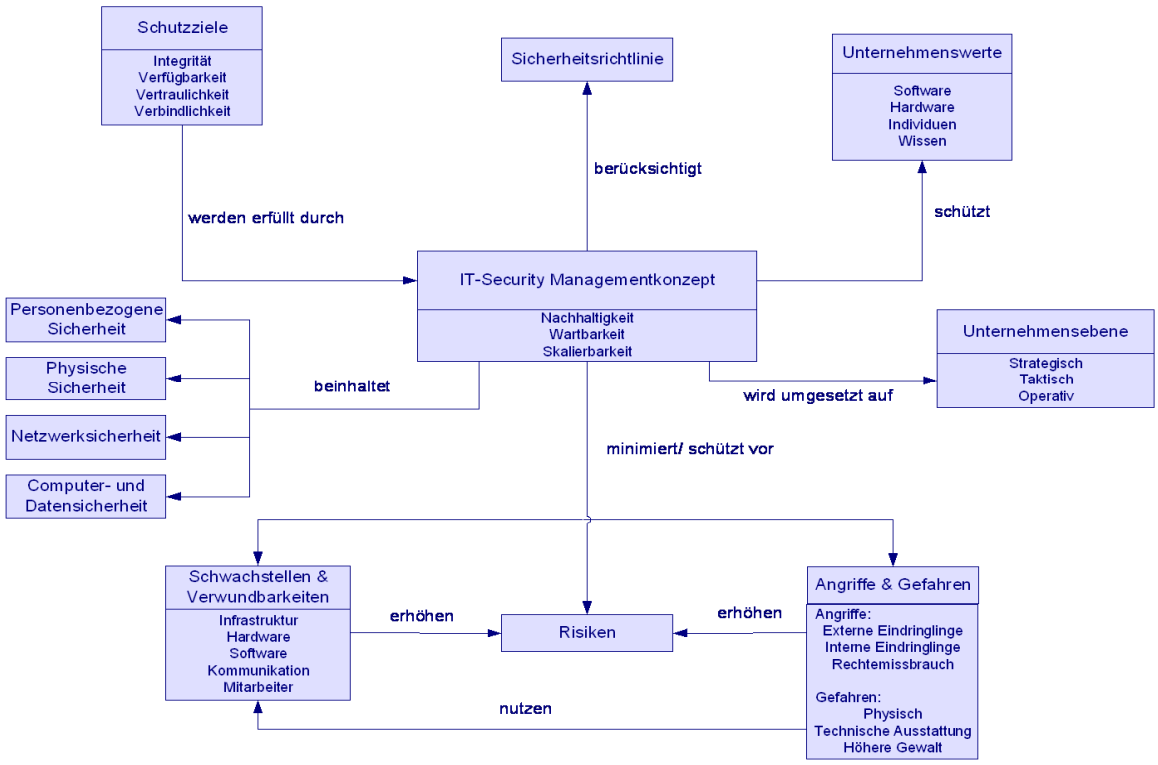


Abbildung 9: Einflussfaktoren des nachhaltigen IT-Security Managementkonzepts [eigene Darstellung]

In Abbildung 9 werden die Zusammenhänge und Abhängigkeiten von sicherheitsorientierten Einflussfaktoren an ein nachhaltiges IT-Security Managementkonzept dargestellt. Als wesentlicher Faktor eines Sicherheitskonzepts sind die Unternehmenswerte (Software, Hardware, Individuen und Wissen) zu schützen. Dies kann nur dann erfolgreich von statten gehen, wenn die Schutzziele unter der Berücksichtigung einer Sicherheitsrichtlinie erfüllt werden.

Die Anwendung des IT-Security Managementkonzepts erfolgt zum einen auf den Unternehmensebenen (strategisch, taktisch und operativ), hat aber zugleich auch technische Dimensionen wie personenbezogene-, physische-, Netzwerk, Computer- und Datensicherheit zu beinhalten.

Durch die Etablierung des Security Managementkonzepts in einem Unternehmen lassen sich Risiken, Schwachstellen, Verwundbarkeiten sowie Angriffe und Gefahren minimieren oder bieten dem Unternehmen zumindest besseren Schutz davor. Dies natürlich nur unter der Voraussetzung, dass die erarbeiteten Anforderungen aus Kapitel 6 bei der Umsetzung mit einfließen.

In Abbildung 10 erhält man nochmals einen zusammenfassenden Überblick über die definierten Anforderungen und ihrer Einordnung auf den verschiedenen Unternehmensebenen. Des weiteren wird dargestellt, dass auf jeder Ebene existierende Planungsansätze und Best Practices herangezogen werden können, die bei der Umsetzung der definierten Anforderungen unterstützend beitragen können und sollen.

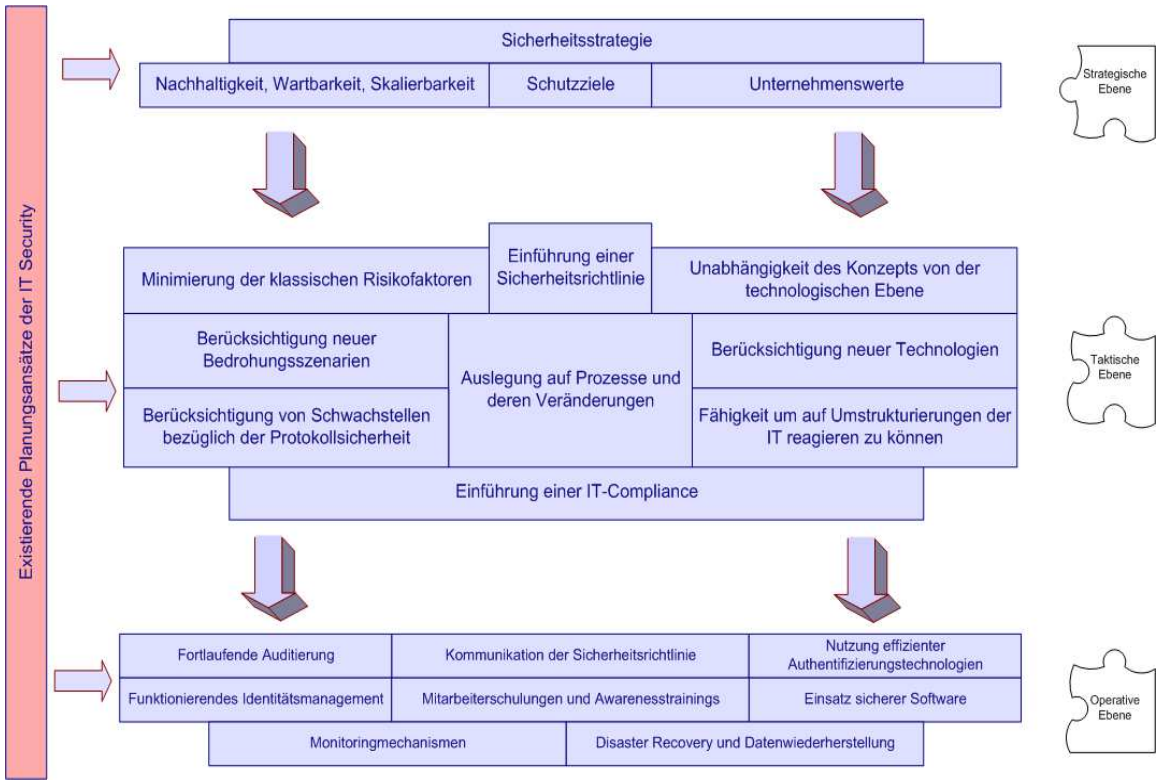


Abbildung 10: Zusammenfassende Darstellung der erarbeiteten Anforderungen nach Unternehmensebenen [eigene Darstellung]

Darunter ist zu verstehen, dass beispielsweise bei der Entwicklung der Sicherheitsstrategie für ein Unternehmen das Kapitel „Sicherheitspolitik“ und „Organisation der Informationssicherheit“ aus der ISO-Normreihe DIN ISO/IEC

27002 (Leitfaden für das Management der Informationssicherheit) herangezogen werden kann. Bezüglich des Umgangs mit den Unternehmenswerten könnte das Kapitel „Management von Vermögenswerten“ aus derselben Normreihe angewandt werden oder auch das Kapitel „Vermögenswerte und Klassifizierung von Informationen“ aus dem österreichischen Informationssicherheitshandbuch.

7.1 Prozess zur Einführung eines nachhaltigen IT-Security Managementkonzepts

Im folgenden Kapitel wird die konkrete Vorgehensweise zur Einführung eines nachhaltigen IT-Security Managementkonzepts beschrieben. Es handelt sich hierbei um einen Prozess, der sich grob in zwei Aufgabengebiete unterteilt.

Das erste Aufgabengebiet bezieht sich auf die Entwicklung des Konzepts unter Berücksichtigung der Anforderungen an die strategische- und taktische Ebene.

Das zweite Aufgabengebiet setzt sich aus Realisierung/ Betrieb zusammen. Eine wesentliche Herausforderung dabei ist, das entworfene Security Konzept in den bestehenden Strukturen eines Unternehmens zu verankern und dann auch umzusetzen. In den Bereich der Realisierung fließen dann auch die Anforderungen der operativen Ebene in das Konzept ein.

Bei der Gestaltung des nachhaltigen IT-Security Managementkonzepts wurde darauf Wert gelegt, den vielfach bewährten PDCA-Zyklus und dessen Vorteile zu integrieren. Er gewährleistet in gewisser Weise unterstützend die grundlegende Anforderung der Nachhaltigkeit und stellt darüber hinaus ein probates Mittel zur kontinuierlichen Verbesserung des Prozesses dar. Im schnelllebigen Themengebiet der IT-Security gilt es, wie bereits mehrfach aufgezeigt, als unerlässlich, sich ständig mit neu aufkommenden Herausforderungen auseinander zu setzen und diese in sein Security Managementkonzept einfließen zu lassen. Die grundlegende Idee war es, bei jedem Durchlauf des Zyklus, einerseits noch zu behebende Mängel im Security Konzept zu beseitigen, zum anderen durch Einarbeitung neuer Erkenntnisse ein höheres Sicherheitsniveau zu erreichen. In Abbildung 11: Prozess zur

Einführung eines nachhaltigen Security Managements [eigene Darstellung] ist ersichtlich, wie der adaptierte PDCA-Zyklus über den gesamten Prozess gelegt wurde.

Das Element „Plan“ des PDCA-Zyklus umfasst den Bereich der Entwicklung des nachhaltigen Security Managementkonzepts, sowie die Analyse und das Aufdecken von eventuellen Verbesserungspotentialen. Das Element „Do“ entspricht in dem vorgestellten Prozess der konkreten Umsetzung des Konzepts bzw. Integration in das Unternehmen. Das Element „Check“ entspricht der Überprüfung des Konzepts auf seine Wirkung in der Praxis. Diese wird beispielsweise im Rahmen von Audits durchgeführt. Aufgrund der gewonnenen Informationen und Ergebnisse greift die Feedback-Schleife, die in diesem Fall dem Element „Act“ entspricht. Das Resultat der Audits kann dazu führen, dass eine weitere IST-Analyse des Unternehmens notwendig ist, die Auswahl existierender Standards und Best-Practices angepasst werden muss oder dass das Sicherheitskonzept überarbeitet werden sollte. In seltenen Fällen ist es möglich, dass im Rahmen von Audits festgestellt wird, dass die Sicherheitsstrategie grundsätzlich zu überdenken ist.

Darüber hinaus wird aus der Abbildung ersichtlich, welche Phasen von der Initiierung durch das Management bis hin zu einer möglichen Zertifizierung durchlaufen werden müssen. In der Spalte „Zuordnung der Anforderungen“ sieht man die in den vorherigen Kapiteln definierten Anforderungen an ein nachhaltiges Security Managementkonzept und zu welchen Phasen diese zugeordnet werden müssen. In der Spalte „Output einzelner Phasen“ wird der zu erwartende Output der einzelnen Phasen abgebildet.

Eine nähere Beschreibung der einzelnen Phasen zur Einführung des nachhaltigen Security Managementkonzepts erhalten Sie in den nächsten Kapiteln. Zusätzlich werden in jeder Phase entsprechende Verweise auf bestehende Standards und Best Practices gegeben, die bei der Umsetzung unterstützend hinzugezogen werden können.

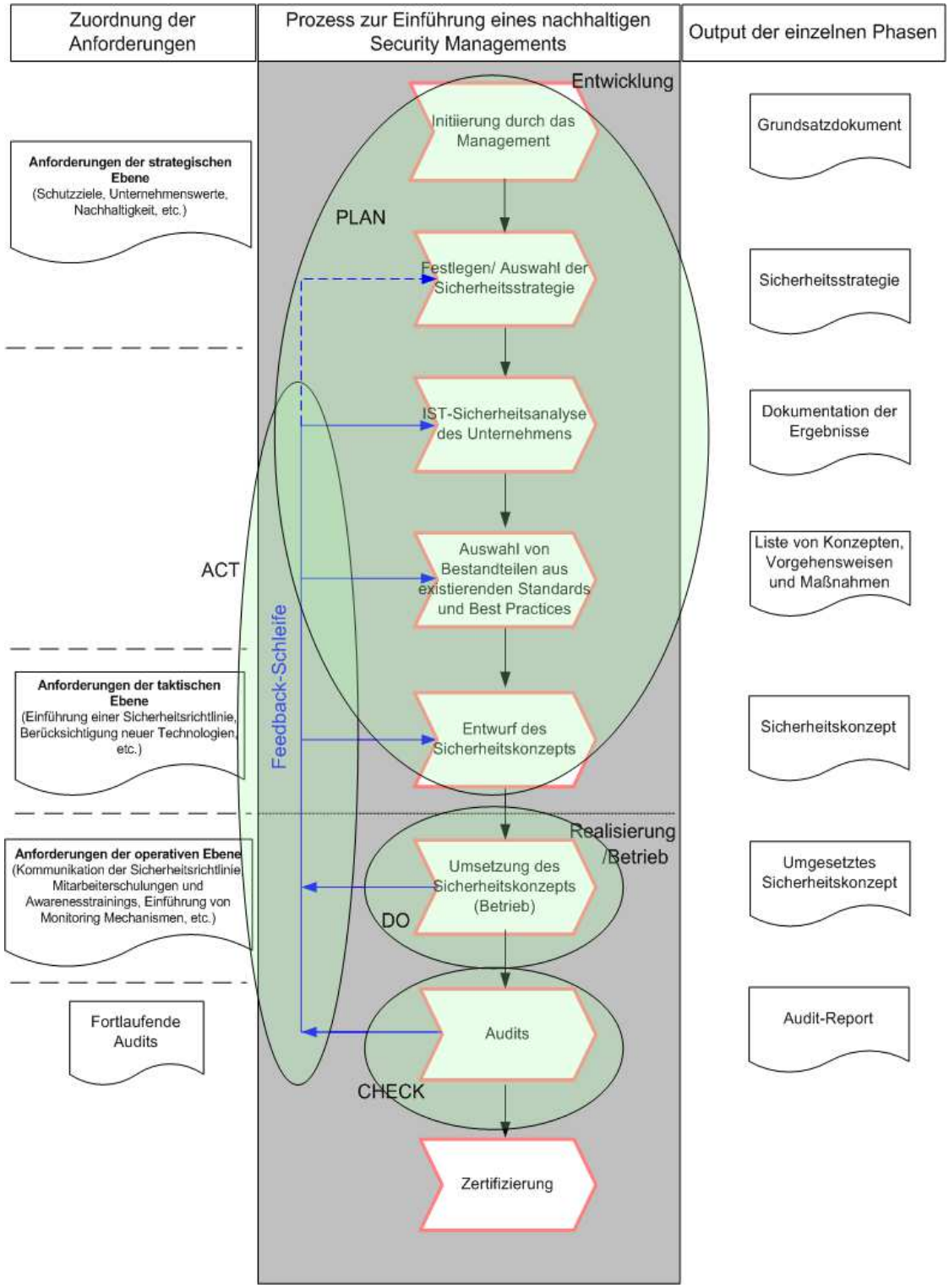


Abbildung 11: Prozess zur Einführung eines nachhaltigen Security Managements [eigene Darstellung]

7.1.1 Initiierung durch das Management

Der Prozess zur Einführung des nachhaltigen Security Managementkonzepts erfolgt durch die Initiierung auf Managementebene. Die grundsätzlichen Rahmenbedienungen werden von den Managementorganen festgelegt bzw. geschaffen.

Dazu zählt zum einen die Definition der Sicherheitsziele, welche durch die Einführung des Security Managementkonzepts erfüllt werden sollen. Jedoch gilt es zu beachten, dass es Grenzen bezüglich der Sicherheit gibt und 100%ige Sicherheit nicht gewährleistet werden kann. Durch unvorhersehbare Verkettungen von Vorfällen kann es immer vorkommen, dass ein nicht erwarteter Schaden eintritt. Die Ziele sollten durch das Management so definiert werden, dass die Risiken auf ein akzeptables Maß gesenkt werden, damit die Ziele in weiterer Folge unter vertretbarem finanziellen, personellen und zeitlichen Aufwand erreicht werden können. [BKÖ10]

Zum anderen müssen zahlreiche organisatorische Maßnahmen getroffen werden. Beispielsweise, jener Zeitpunkt, bis zu dem die Etablierung des Managementkonzepts im Unternehmen erfolgt sein sollte; welche Mitarbeiter für das Projektmanagement zur Einführung und Etablierung verantwortlich sind und als Ansprechpersonen dienen; aber natürlich auch die Fragestellungen, ob neue Mitarbeiter (z.B. Security-Experten) eingestellt, externe Berater hinzugezogen werden und aus welchen Abteilungen Mitarbeiter mit einbezogen werden müssen. Ein Stichwort hierzu ist die Planung des Personal- und Ressourcenmanagements. [BKÖ10]

Da das entworfene Security Managementkonzept auch als ein sich zyklisch wiederholender Sicherheitsprozess angesehen werden kann, wie man später sehen wird, handelt es sich bei den getätigten Entscheidungen auf Managementebene um Handlungen, die langfristige und nachhaltige Auswirkungen für das Unternehmen haben werden. Die zu tätigenden organisatorischen Maßnahmen des Sicherheitsprozess hängen natürlich von

der Größe und den Aufgaben des Unternehmens ab und werden sich daher auch in seiner Komplexität individuell unterscheiden.

Zusammenfassend sollten als **Output** der Initiierungsphase zumindest folgende Schlüsselelemente in Form eines Grundsatzdokuments hervorgehen:

- **Definierung der grundsätzlichen Anforderungen und Ziele bzw. des zu erwartenden Outputs nach Einführung des Security Managementkonzepts**
- **Festlegung eines Projekt- und Zeitplans zur Etablierung des Managementkonzepts und zur langfristigen Verankerung im Unternehmen**
- **Festlegung der Rollen und verantwortlichen Personen**
- **Bereitstellung von notwendigen Ressourcen**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Definierung der Ziele und grundsätzlichen Anforderungen	Kapitel 2,3,6 des österreichischen Sicherheitshandbuch Kapitel 4 des BSI-Standard 100-1 – Management für Informationssicherheit (ISMS) Kapitel 5 des ISO/IEC 27001:2005 – Informationstechnologie – Sicherheitstechnik (ISMS – Anforderungen)
Organisatorische Maßnahmen (z.B. Rollen und Ressourcenmanagement)	Kapitel 3.2 d. österr. Sicherheitshandbuch Kapitel 5,6 des BSI-Standard 100-1 – Management für Informationssicherheit (ISMS) Kapitel 5.2 des ISO/IEC 27001:2005 – Informationstechnologie – Sicherheitstechnik (ISMS – Anforderungen)

Festlegung eines Projekts- und Zeitplans	PMBOK Guide

7.1.2 Festlegung/ Auswahl der Sicherheitsstrategie

Im zweiten Schritt zur Einführung eines nachhaltigen Security Managementkonzepts gilt es, auf strategischer Ebene eine durchgehende Sicherheitsstrategie für das Unternehmen zu entwerfen. Die Entwicklung dieser hat unter Berücksichtigung der von der Managementebene vorgegebenen Ziele und Rahmenbedingungen zu erfolgen. Des Weiteren gilt es in diesem Schritt als sinnvoll, die Managementebene mit einzubeziehen und als eine Art Kontrollorgan für die entwickelte Sicherheitsstrategie einzusetzen. Dadurch wird von Anfang an gewährleistet, dass die festgelegten Ziele der Managementebene vollständig in die Strategie einfließen und sowohl ressourcen- als auch kosten- und zeitintensive Anpassungsmaßnahmen zu einem späteren Zeitpunkt vermieden werden können.

Pauschal kann nicht entschieden werden, wie die Security Strategie auszusehen hat, da diese unter anderem von der Art des Unternehmens abhängt und natürlich auch auf welchen Unternehmensbereich sie ausgelegt werden soll. Im Kapitel 6.1.3 wurden die wesentlichen Merkmale zur Einführung einer durchgehendenden Sicherheitsstrategie beschrieben. Nochmals erwähnt sei, dass diese in jedem Fall die elementaren Ziele und die Festlegung der Eckpfeiler der IT-Security umfassen muss. Zu diesen zählen die Einhaltung der Schutzziele, Schutz der Unternehmenswerte, sowie das Bestreben, dass das Security Managementkonzept den Prämissen der Nachhaltigkeit, Wartbarkeit und Skalierbarkeit entspricht.

Eine weitere wesentliche Anforderung an ein nachhaltiges IT-Security Managementkonzept sollte ebenfalls in der Sicherheitsstrategie verankert werden, obwohl sie erst zu einem späteren Zeitpunkt auf taktischer Ebene konkret umgesetzt wird. Hierbei handelt es sich um den Bedarf zur Einführung einer Sicherheitsrichtlinie.

Darüber hinaus sollten beim Entwerfen der Sicherheitsstrategie existierende Planungsansätze zur IT-Security unbedingt berücksichtigt und verankert werden. Es gilt zu untersuchen, welche Standards und Best-Practices es gibt, welche Charakteristika diese aufweisen und wie sie in die Sicherheitsstrategie einfließen können.

Output dieser Phase sollte eine auf das Unternehmen ausgelegte Sicherheitsstrategie sein, die zumindest folgende Punkte umfasst:

- **Verankerung der Prämissen der Nachhaltigkeit, Wartbarkeit, Skalierbarkeit**
- **Einhaltung der Schutzziele zum Schutz der Unternehmenswerte**
- **Verankerung des angestrebten Sicherheitsniveaus im Unternehmen in der Sicherheitsstrategie, basierend auf den definierten Anforderungen und Zielen der Managementebene**
- **Security Managementkonzept wird als Prozess in das Unternehmen integriert**
- **Bedarf zur Einführung einer Sicherheitsrichtlinie**
- **Bedarf eines Sicherheitskonzepts auf Basis bestehender Standards und Best Practices**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Aufbau einer Sicherheitsstrategie	Kapitel 5 des österreichischen Sicherheitshandbuch Kapitel 3.1, 3.2 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise Kapitel 5 des ISO/IEC 27002:2005 –

	Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)

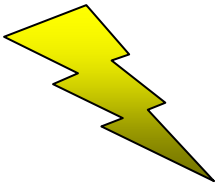
7.1.3 IST-Sicherheitsanalyse des Unternehmens

Die Hauptaufgabe dieser Phase ist es, eine IST-Sicherheitsanalyse des Unternehmens durchzuführen. Die zentrale Herausforderung hierbei ist, das derzeitige Sicherheitsniveau zu analysieren. Dazu zählen die Analyse der Unternehmensorganisation, sowie bereits getätigte oder noch zu treffende Maßnahmen bezüglich der IT-Security zu identifizieren. Darüber hinaus gilt anhand der Analyse zu klären, welche Anforderungen der zuvor entworfenen Sicherheitsstrategie aus der vorhergehenden Phase bereits im Unternehmen umgesetzt wurden.

Bei der IST-Sicherheitsanalyse sind beispielsweise folgende Punkte relevant und zu berücksichtigen:

- **Analyse der Nutzer- und Anwenderumwelt**
    - Organisationsaufbau, Personelle Sicherheit (Regelungen für Mitarbeiter, Dienstvorschriften, Gesetze, Richtlinien usw.)
- **Analyse der physischen und umgebungsbezogenen Sicherheit**
    - Überprüfung baulicher und infrastruktureller Maßnahmen
- **Erfassen existierender IT-Systeme und ähnlicher Objekte**
- **Erfassen der vorhanden IT-Ausrüstung**
- **IST-Aufnahme des Netzes und der Netzsicherheit**
- **Auf welche Standards und Best-Practices wurde bisher gesetzt**

Des Weiteren führt die IST-Sicherheitsanalyse im Normalfall auch zu:



- Aufreten bis dahin nicht bekannter Schwachstellen und deren Ursachen.
- Ermittlung von existierenden Bedrohungen und nicht beseitigten Verwundbarkeiten in Form von **Bedrohungs- und Risikoanalysen.**

Nicht unwesentlich für die Auswirkungen bzw. Resultate der IST-Sicherheitsanalyse ist, ob das Unternehmen sich bereits auf bestehende Standards und Best-Practices stützt. Es ist davon auszugehen, dass die Ergebnisse der Analyse nach weniger Anpassungen verlangen, wenn bereits ein konzeptionelles Vorgehen bezüglich der IT-Sicherheit vorliegt. Des Weiteren sollte bei der IST-Analyse überprüft werden, ob und welche Tätigkeiten gesetzt wurden, um den Anforderungen aus Kapitel 6 an ein nachhaltiges IT-Security Managementkonzepts zu entsprechen.

Als **Output** dieser Phase sollten folgende Punkte hervorgehen:

- **Dokumentation der Ergebnisse der IST-Sicherheitsanalyse**
- **Dokumentation der Abweichungen gegenüber den Zielen und Anforderungen der entworfenen Sicherheitsstrategie**
- **Dokumentation der neu entdeckten Schwachstellen**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema : IST- Sicherheitsanalyse	**Standards & Best Practices**
IST-Aufnahme der Vermögenswerte des Unternehmens	Kapitel 7 des österreichischen Sicherheitshandbuch Kapitel 4 - 4.5 des BSI-Standard 100-2 – IT-

	Grundschutz-Vorgehensweise Kapitel 7 des ISO/IEC 27002:2005 – Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)
Risikoanalysestrategien	Kapitel 4 des österreichischen Sicherheitshandbuch Kapitel 4.6 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise Bzw. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz Kapitel 4 des ISO/IEC 27002:2005 – Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)

7.1.4 Auswahl von Bestandteilen existierender Standards und Best-Practices

Dieser Schritt zur Umsetzung eines nachhaltigen IT-Security Managementkonzepts umfasst die Auswahl von Vorgehensweisen aus bestehenden Security-Standards und Best Practices. Da diese teilweise sehr umfangreich sind, gilt es zu entscheiden, ob ein ganzer Standard inhaltlich vollständig umgesetzt wird, oder nur einzelne Teile herausgenommen werden. Dies ist natürlich vom Typ des Unternehmens abhängig und der dazugehörigen Sicherheitsstrategie, sowie davon, welche Erkenntnisse bei der IST-Analyse erlangt wurden. Grundsätzlich sollen in dieser Phase durch die geeignete Auswahl aus bestehenden Standards und Best Practices entdeckte Schwachstellen während der IST-Analyse eliminiert bzw. wenn möglich minimiert werden. Hinzu sollen, falls Abweichungen bezüglich der Anforderungen der entworfenen Sicherheitsstrategie und deren Ziele bestehen, diese durch geeignete Auswahl beseitigt werden.

Der **Output** dieses Schritts umfasst folgenden Punkt:

- **Konkrete Liste von Konzepten, Vorgehensweisen oder Maßnahmen aus bestehenden Standards und Best-Practices zur Verringerung und Beseitigung von Sicherheitsdefiziten.**

Folgende Standards können unterstützend zur Umsetzung in dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Auswahl von Standards und Best Practices	Österreichisches Sicherheitshandbuch Version 3.1.000 22. November 2010
	BSI-Standard 100-1 – Managementsysteme für Informationssicherheit (ISMS)
	BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise
	BSI-Standard 100-3 – Risikoanalyse auf der Basis von IT-Grundschutz
	BSI – IT-Grundschutz-Kataloge
	ISO/IEC 2700x Reihe – Information Security
	COBIT – Standard
	ITIL – Sammlung
	Common Criteria – Zur Bewertung und Zertifizierung der Sicherheit von Computersystemen in Hinblick auf Datensicherheit

7.1.5 Entwurf des Sicherheitskonzepts

Dieser Bereich beschäftigt sich mit dem konkreten Entwurf eines Sicherheitskonzepts. Es gilt, die Bestandteile, welche aus existierenden Planungsansätzen und Best Practices übernommen wurden, in entsprechender Form umzusetzen. Die Berücksichtigung und Integration der identifizierten Sicherheitsanforderungen an die taktische Ebene ist in diesem Schritt

unbedingt vorzunehmen, um die korrekte Etablierung des nachhaltigen IT-Security Managementkonzepts zu gewährleisten.

Nachstehend wird nochmals kurz beschrieben, welche konkreten Anforderungen in dieser Phase neben den individuell ausgewählten Bestandteilen aus Standards und Best-Practices berücksichtigt werden müssen, falls dies nicht bereits der Fall im Unternehmen war:

- **Minimierung klassischer Risikofaktoren:** mittels zuvor getätigter Risikoanalysen, sowie geeigneter Maßnahmen aus Standards und Best-Practices
- **Einführung einer Sicherheitsrichtlinie:** dient als eine Art Grundsatzdokument bezüglich der Sicherheit im Unternehmen
- **Einführung einer IT-Compliance:** Zur Gewährleistung der Gesetzeskonformität (gesetzliche Vorgaben). Weiters kann überprüft werden ob unternehmensintern festgelegte regulative Vorgaben (Richtlinien, Normen, Standards, Best-Practices) eingehalten werden
- **Unabhängigkeit des Konzepts von der technologischen Ebene:** Das Konzept ist so auszulegen, dass es keine Einschränkungen bezüglich der einzusetzenden Technologien gibt. Das heißt, Beschränkungen des Konzepts auf bestimmte Hard- oder Software sollten vermieden werden. Nur so kann garantiert werden, dass neue Technologien problemlos integriert werden können. Jedoch sollte auf eine Kompatibilität der Technologien geachtet werden, um keine zusätzlichen Verwundbarkeiten entstehen zu lassen.
- **Berücksichtigung neuer Technologien:** Beachten, dass es die Möglichkeit gibt, neue Technologien zu integrieren, speziell in Hinblick auf Trends wie IT-Consumerization, Cloud Computing und Virtualisierung.

- **Auslegung auf Prozesse und deren Veränderungen:** IT-Security von Beginn an in die Entwicklung von Prozessen mit einbeziehen; gegebenfalls Schutzbedarfsanalysen für die Prozesse durchführen; Kernprozesse identifizieren und entsprechend schützen, usw.

- **Fähigkeit, auf Umstrukturierungen der IT reagieren zu können:** Festlegen eines Maßnahmenkatalogs, wie die Vorgehensweise bei Umstrukturierungen der IT zu sein hat.

- **Berücksichtigung neuer Bedrohungsszenarien:** Wie bereits beschrieben, gibt es eine Vielzahl von Gründen zum Auftreten neuer Bedrohungsszenarien. Diese sind unbedingt zu berücksichtigen und wenn nötig, präventive Maßnahmen zu ergreifen. Zum einen kann hierbei auf bestehende Best-Practices zurückgegriffen werden, zum anderen wird eine ständige aktive Beobachtung (Monitoring) hinsichtlich der zu treffenden Maßnahmen notwendig sein.

- **Berücksichtigung von Schwachstellen bezüglich der Protokollsicherheit:** Weiterentwicklungen der Protokolle BGP und DNS, in Zukunft wenn möglich einsetzen. Stichwort: *S-BGP(Secure Border Gateway Protocol), TSIG (Transaction Signatures)* und *DNSSEC (DNS-Security)*, um die DNS Sicherheit zu garantieren. Etwaige Sicherheitsvorfälle können auf Schwächen in der Protokollsicherheit zurückzuführen sein.

Der **Output** dieser Phase sollte sein:

- **Ein Entwurf des Sicherheitskonzepts basierend auf Standards und Best-Practices unter Berücksichtigung der identifizierten Anforderungen, sowohl auf strategischer als auch auf taktischer Ebene.**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	Standards & Best Practices
Erstellung eines Sicherheitskonzepts	Kapitel 2,8,9,12,15 des österreichischen Sicherheitshandbuch Kapitel 4,5 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise Kapitel 4 des ISO/IEC 27001:2005 - Informationstechnologie – Sicherheitstechnik (ISMS – Anforderungen) Kapitel 8,9,10,11,15 des ISO/IEC 27002:2005 – Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)

7.1.6 Umsetzung des Sicherheitskonzepts (Betrieb)

In dieser Phase muss überprüft werden, ob die allgemeinen Anforderungen aus den existierenden Standards und Best Practices umgesetzt wurden, sofern man sich entschieden hat, das Sicherheitskonzept mittels dieser aufzubauen. Ziel ist es, die Aufrechterhaltung des erreichten Sicherheitsniveaus sicherzustellen und die Sicherheitseinrichtungen zu warten und zu administrieren. Parallel dazu wird vorausgesetzt, dass die individuellen Anforderungen der taktischen Ebene an ein nachhaltiges Security Managementkonzept berücksichtigt wurden. Dies kann im Rahmen eines Security Compliance Checking erfolgen. Dieses beinhaltet eine Überprüfung der getätigten Maßnahmen auf Übereinstimmung mit der Sicherheitsstrategie. Ist dies nicht der Fall, müssen entsprechende Maßnahmen und eventuelle Nachbesserungen in den vorhergehenden Phasen getätigt werden.

Zusätzlich müssen in dieser Phase die identifizierten Anforderungen an die operative Ebene berücksichtigt werden. Nachstehend ist aufgelistet, um welche es sich dabei handelt.

- **Kommunikation der Sicherheitsrichtlinien:** Kommunikation der Richtlinien an die Mitarbeiter; Formulierungen sind entsprechend der

Zielgruppen anzupassen. Aufzeigen, welche Konsequenzen ein Nichtbeachten der Richtlinien mit sich bringt

- **Mitarbeiterschulungen und Awarenesstrainings:** Durchzuführen, um die Mitarbeiter für das Thema IT-Sicherheit zu sensibilisieren; Mitarbeiter müssen aktiv zur Sicherheit beitragen; Vermittlung der notwendigen Fachkenntnisse, damit dies auch möglich ist

- **Nutzung von effizienten Authentifizierungstechnologien:** Konkrete Umsetzung von Authentifizierungstechnologien, sowohl auf Hard- als auch auf Softwareebene

- **Umsetzung eines funktionierenden und nachhaltigen Identitätsmanagement:** spielt eine wesentliche Rolle zum Schutz sensibler Daten; Beeinflusst wesentliche Teile des Themengebiets Security, z.B. Schutz der Unternehmenswerte, gesetzliche Anforderungen (Compliance), Einschränkung neuer Bedrohungsszenarien; Stichwort: Federal Identity Management

- **Einsatz sicherer Software:** Zurückgreifen auf sichere und ausgereifte Softwarelösungen, um keine zusätzlichen Verwundbarkeiten für das Unternehmen zu schaffen

- **Einführung von Monitoringmechanismen:** ist von Bedeutung, da eigentlich nie eine vollständige IT-Security gewährleistet werden kann; Wesentlich ist auch die Beobachtung von Weiterentwicklungen in diesem Sektor

- **Umsetzung von Disaster Recovery- und Datenwiederherstellungsmaßnahmen:** Treffen von Maßnahmen, um einen Fortbestand der regulären Geschäftsabläufe zu ermöglichen; garantiert, dass die Ausfallzeiten der IT möglichst gering gehalten werden können

Der **Output** dieser Phase sollte sein:

- **Ein konkretes, vollständiges und bereits umgesetztes Sicherheitskonzept basierend auf Standards und Best-Practices unter Berücksichtigung der identifizierten Anforderungen, sowohl auf strategischer, taktischer als auch operativer Ebene.**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Umsetzung/ Betrieb Sicherheitskonzept	Kapitel 10,11,12,13,14 des österreichischen Sicherheitshandbuch Kapitel 5 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise BSI-Standard 100-4 – Notfallmanagement Kapitel 4.2.2-4.2.4 des ISO/IEC 27001:2005 - Informationstechnologie – Sicherheitstechnik (ISMS – Anforderungen) Kapitel 10,11,12,13,14 des ISO/IEC 27002:2005 – Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)

7.1.7 Audits

Die Durchführung von Audits dient zur Überprüfung, ob die definierten Ziele, Anforderungen, Vorgaben und Maßnahmen bezüglich der IT-Sicherheit entsprechend erfüllt wurden. Deshalb stellen sie selbst auch eine wesentliche Anforderung an ein nachhaltiges Security Managementkonzept dar. Es sei nochmals erwähnt, dass mittels regelmäßig durchgeführter Sicherheitsaudits die in dieser Arbeit definierten Anforderungen an die IT-Security auf ihre Wirksamkeit im Unternehmen geprüft werden können. Beispielsweise kann überprüft werden, ob wirkliche alle Vorschriften der IT-Compliance erfüllt sind, ob bestehende Maßnahmen zur Aufrechterhaltung des Sicherheitsniveaus nach

wie vor geeignet sind, ob diese korrekt umgesetzt werden und auch von allen Beteiligten eingehalten werden. Die Durchführung sollte von der internen Revision oder externen Partnern erfolgen.

Insbesondere, wenn im Laufe der Sicherheitskonzepterstellung nur Teile von Standards oder der Best Practices eingeführt wurden, ist eine Auditierung sinnvoll, da eine Überprüfung durch eine Zertifizierung nicht möglich ist. Prinzipiell ist es zu empfehlen, sich an etablierten Standards und Best Practices zu orientieren und diese auf sein Unternehmen auszulegen. Ergänzend sollten die identifizierten Anforderungen an ein nachhaltiges Security Managementkonzept unbedingt berücksichtigt werden und in weiter Folge auch auf allen Ebenen in das Konzept einfließen.

Der **Output** dieser Phase sollte sein:

- **Ein Audit-Report mit Ergebnissen, ob die definierten Ziele, Anforderungen, Vorgaben und Maßnahmen bezüglich der IT-Sicherheit entsprechend erfüllt wurden, auch hinsichtlich ihrer Wirksamkeit. Darüber hinaus sollte hervor gehen, ob die Sicherheitsziele, die Strategie und das Konzept aktuell noch geeignet sind. Die Ergebnisse des Audits können in Form von Verbesserungen anschließend in das nachhaltige Security Managementkonzept einfließen.**

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Audits	Kapitel 3.3 des österreichischen Sicherheitshandbuch Kapitel 6 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise Kapitel 6,7,8 des ISO/IEC 27001:2005 - Informationstechnologie – Sicherheitstechnik (

	ISMS – Anforderungen) Kapitel 15 des ISO/IEC 27002:2005 – Informationstechnologie – Sicherheitstechnik (Leitfaden für das Management der Informationssicherheit)

7.1.8 Zertifizierung

Die letzte Phase zur Einführung eines nachhaltigen IT-Security Managementkonzept beschäftigt sich mit der Zertifizierung. Nach Einführung und Auditierung eines Sicherheitskonzepts auf Basis von Standards oder Best Practice-Ansätzen kann eine Zertifizierung stattfinden, sofern der Standard dies ermöglicht. Die Zertifizierung bescheinigt, dass eingeführte Bestandteile bzw. Prozesse, wie in einem anerkannten Standard gefordert, eingeführt und umgesetzt wurden.

Folgende Kapitel aus bestehenden Standards können unterstützend zur Umsetzung dieser Phase herangezogen werden:

Thema	**Standards & Best Practices**
Zertifizierung nach ISO 27001	Kapitel 7 des BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise

8 Überprüfung der Praxistauglichkeit des entworfenen IT-Security Managementkonzepts in Kooperation mit der Via Donau

Die Überprüfung der Praxistauglichkeit des entworfenen Konzepts erfolgt im Rahmen einer Fallstudie in Zusammenarbeit mit der „via donau – Österreichische Wasserstraßen-Gesellschaft mbH“, welche im Jahr 2005 vom österreichischen Bundesministerium für Verkehr, Innovation und Technologie (bmvit) zur Erhaltung und Entwicklung der Wasserstraße Donau gegründet wurde. [ViaD11]

Die Kernkompetenzen der „via donau“ liegen im Infrastrukturmanagement der österreichischen Wasserstraßen, Verkehrsmanagement auf der österreichischen Donau, Entwicklung der Binnenschifffahrt und Hochwasserschutz. [ViaD11] Dazu zählen vielseitige Aufgaben wie die Herstellung und Instandhaltung der Wasserstraßeninfrastruktur, ökologische Wasserbau- und Renaturierungsprojekte, Betrieb der Donauschleusen, Betrieb von DoRIS (Donau River Information Services) – ein Informations- und Managementsystem für die Schifffahrt auf der Donau – Maßnahmen zur Verbesserung und Erhaltung des Hochwasserschutzes, sowie Anstrengungen zur Verbesserung der Rahmenbedienungen für die Donauschifffahrt, um die umweltfreundliche und kostengünstige Wasserstraße Donau attraktiver und moderner zu machen. [ViaD11]

In Abbildung 12 ist das Organigramm der „via donau“ dargestellt. Es handelt sich um ein Unternehmen mittlerer Größe und umfasst ca. 270 Mitarbeiter, welche in Form von Teams in Abteilungen unterhalb der Geschäftsführung etabliert sind. Die Überprüfung der Praxistauglichkeit des Security Managementkonzepts erfolgt konkret in Zusammenarbeit mit dem Team der IT der Abteilung Verkehrsmanagement.

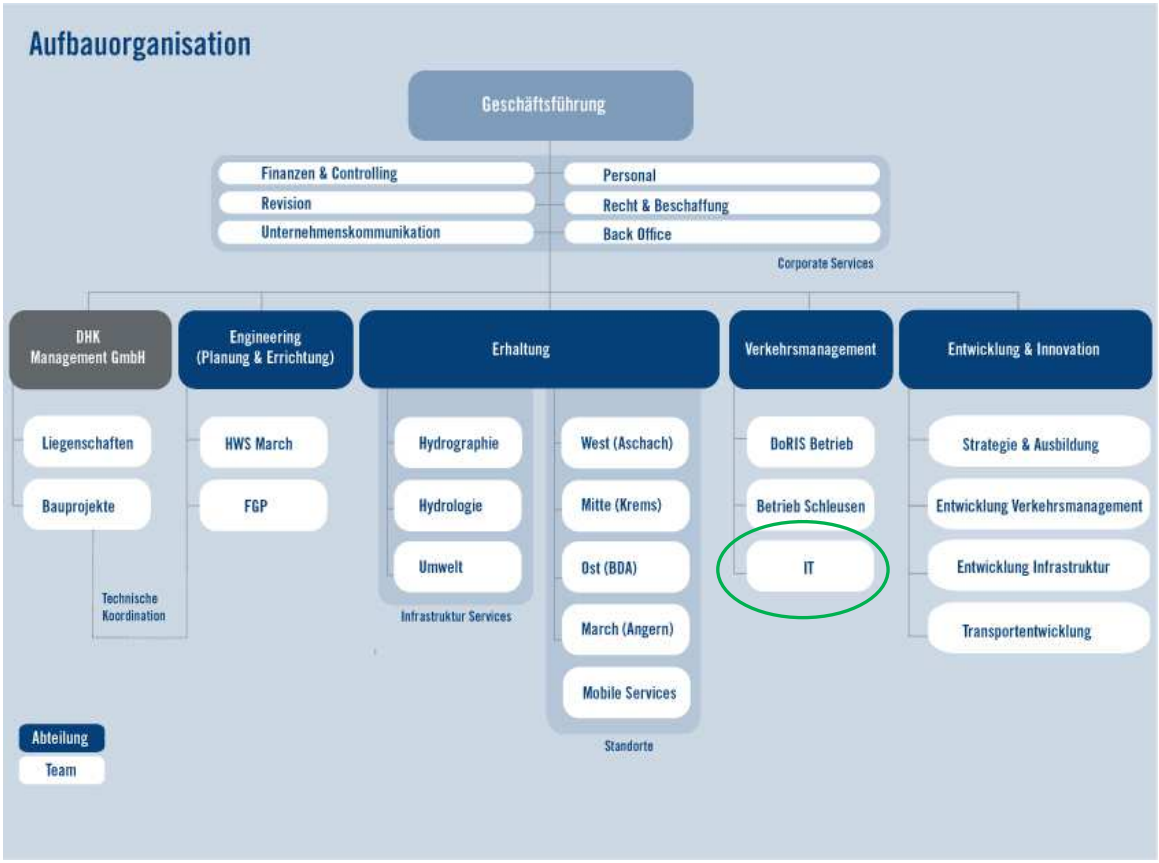


Abbildung 12: Organigramm der via donau [ViaD11]

Die Erwartungshaltung der „via donau“ bezüglich der Case Study liegt darin, dass sich bei der Überprüfung auf Praxistauglichkeit des Prozesses zur Einführung eines nachhaltigen IT-Security Managementkonzepts, neue Erkenntnisse und Empfehlungen ergeben, die einen Schritt zur Verbesserung der IT-Security beitragen können. Ein weiteres Ziel ist es, die gewonnenen Erkenntnisse in Form einer Sammlung von Ratschlägen an das Unternehmen weiter zu geben und somit die Möglichkeit zu bieten, diese zukünftig konkret in ihr Sicherheitsmaßnahmenkonzept einfließen zu lassen.

In den nun folgenden Kapiteln erfolgt eine Überprüfung auf Praxistauglichkeit des nachhaltigen IT-Security Managementkonzepts bzw. der Vorgehensweise zur Einführung desselbigen. Dies erfolgt in Kooperation mit IT-Team der „via donau“.

8.1 Prozess zur Einführung eines nachhaltigen IT-Security Managements bei der via donau

In den folgenden Kapiteln werden die einzelnen Phasen des Prozesses zur Einführung eines nachhaltigen IT-Security Managementskonzepts auf die „via donau“ angewandt. Anzumerken ist, dass die Phase der „Initiierung durch das Management“ nicht berücksichtigt wird, da bereits ein IT-Managementkonzept im Unternehmen verankert ist, welches den Bereich der IT-Security beinhaltet. Hauptaugenmerk wird auf die Phasen „Festlegen/ Auswahl der Sicherheitsstrategie“ bis hin zu möglichen „Audits“ gelegt. Prinzipiell erfolgt in jeder Phase eine Überprüfung, inwiefern die definierten Anforderungen zur Einführung eines nachhaltigen IT-Security Konzepts bei der „via donau“ erfüllt sind. Daraus resultierend ergeben sich dann die Handlungsempfehlungen für das Unternehmen.

8.1.1 Festlegen/ Auswahl der Sicherheitsstrategie

Beim Festlegen/ Auswahl der Sicherheitsstrategie wird als Grundlage auf die bestehende IT-Strategie der „via donau“ zurückgegriffen und um notwendige Aspekte ergänzt, damit sie schlussendlich den Anforderungen eines nachhaltigen IT-Security Managementkonzepts entspricht. Dazu werden im nachfolgenden Kapitel die wichtigsten Bestandteile der IT-Strategie zusammengefasst.

8.1.1.1 Derzeitige IT-Strategie der via donau

Die derzeitige IT-Strategie der „via donau“ bezieht sich auf **strategische Vorgaben** für den **Bereich der Informations- und Kommunikationstechnik** für den Zeitraum 2010-2016. Sie beinhaltet sowohl den derzeitigen Stand und die geplanten Anpassungen der IT-Prozesse, Organisation, sowie der IT-Applikationen und IT-Infrastruktur. Darüber hinaus wurden im Speziellen die Ergebnisse der im 2. Quartal 2010 durchgeführten IT-Organisationsanalyse, sowie mittelfristige Vorgaben der Geschäftsführung für den Zeitraum bis 2012 berücksichtigt. [VW10]

Gemäß der IT-Strategie werden folgende wesentliche Prinzipien und Ziele berücksichtigt [VW10]:

- Ausrichtung auf die Anforderungen der Kernprozesse des Unternehmens
- Einsatz geeigneter und zeitgemäßer Applikationen sowie einer kostenbewussten und sicheren IT-Architektur und IT-Infrastruktur mit Fokus auf Ausfallsicherheit und Verfügbarkeit
- Optimierung der Service-Qualität durch „Key-User Konzept“
- IT-Betriebsbereich (im Folgenden als zentrale IT – ZIT bezeichnet) als kundenorientierter Geschäftspartner der Fachbereiche. Dies soll durch verstärkte Einbindung des ZIT (zentrales IT-Team) in die Planungen, durch partnerschaftliches und proaktives Handeln und funktionierende Kommunikation erreicht werden
- IT-Governance als Managementinstrument mit Entscheidungsgremien, definierten Prozessabläufen und Richtlinien
- strukturiertes Change-Management zur Minimierung der IT-Risiken
- kontrolliertes Outtasking
- standardisierte HW- und SW-Ausstattung
- Ausnutzen von Synergien zwischen den Teams IT und DoRIS-Betrieb

Weiters umfasst die IT-Strategie jene **Leistungen der IT**, die zur Erreichung der Fachbereichsziele dienen, sowie die Grundsätze, die es bezüglich der IT-Architektur und Applikationslandschaft zu berücksichtigen gilt.

Ein Teil der IT-Strategie bezieht sich auf die für die „via donau“ entworfene **Infrastrukturstrategie**. Diese beinhaltet die nötigen Basisdienste und Basistechnologien zur Bereitstellung aller IT-Dienste (Server, Betriebssysteme, Netzwerkkomponenten und – Protokolle, sowie Datei- und Storage- Dienste). Des Weiteren werden das prinzipielle Ziel und die Grundsätze der Infrastrukturstrategie erläutert.

Bei der **Prozessgestaltung der IT** orientiert sich das Unternehmen am Referenzmodell COBIT, sowie auch am Rahmenwerk ITIL für ein systematisches Vorgehen zum Management von IT-Services. Der Detaillierungsgrad entspricht in der Größe und Komplexität den Ansprüchen der „via donau“, welche in Organisationshandbüchern und Richtlinien festgelegt sind.

Das **Organisationshandbuch für Benutzer**, sowie ergänzende Richtlinien beinhalten Vorgaben für die Benutzung und den Umgang mit den vom ZIT zur Verfügung gestellten IT-Services, um deren Verfügbarkeit und Sicherheit zu gewährleisten. Dies umfasst im Wesentlichen Punkte zur Benutzung der Infrastruktur, Unterstützung der Benutzer (Helpdesk), Verfügbarkeit der Applikationen (Service Levels), Datensicherung und –wiederherstellung, Wartungsfenster, Sicherheitsrichtlinien (Passwörter, Netzwerk, usw.) und eine Richtlinie zur Internet-, Email und Datennutzung.

Das **Organisationshandbuch für das ZIT** umfasst deren Unterstützungsprozesse und Aufgaben, sowie Regeln und Verfahren zur Erfüllung ihrer Aufgaben. Insbesondere werden das Configuration-Management, Incident-Management, Problem-Management, Change-Management, Data- Management, Security-Management, Asset- und Lizenz-Management und das Disaster & Recovery Management definiert. Darüber hinaus sind im Handbuch auch die nötigen Tools bzw. Dokumentationen zur Unterstützung der Prozesse beschrieben sowie die Zuständigkeiten für die einzelnen Aufgaben festgelegt.

Verfügbare **Betriebshandbücher** beinhalten die operativen Aufgaben für die Betriebsführung und Systemadministration. Sie dienen als Arbeitsgrundlage für den täglichen Routinebetrieb mit Empfehlungen zum Vorgehen bei Problemen oder Notfällen.

Zusätzlich dazu gibt es eine ständig **gepflegte Dokumentation der IT-Infrastruktur und Applikationslandschaft**.

8.1.1.2 Empfehlungen zur Schaffung einer IT-Strategie unter Berücksichtigung zusätzlicher Sicherheitsaspekte

Zu Beginn sei erwähnt, dass es bei der „via donau“ keine eigens entwickelte Sicherheitsstrategie gibt. Jedoch sind im Zuge der Entwicklung der IT-Strategie prinzipiell eine Vielzahl von sicherheitsrelevanten Aspekten einbezogen worden, die für eine Sicherheitsstrategie ebenfalls erforderlich sind.

Beispielsweise wurden die **grundsätzlichen Anforderungen und Ziele (auch Sicherheitsziele)** der IT unter Berücksichtigung der Vorgaben der Geschäftsführung festgehalten. Das Rollen- und Ressourcenmanagement für den Bereich der IT ist ebenfalls verständlich beschrieben und definiert, das **angestrebte Sicherheitsniveau**, welches man erreichen will, wurde festgehalten und die **Einhaltung der Schutzziele** (Authentizität, Integrität und Vertraulichkeit der Daten) wurden verdeutlicht. In gewisser Weise wurde zu den Themen **Nachhaltigkeit, Wartbarkeit und Skalierbarkeit** Bezug genommen, auch wenn diese Schlagwörter nicht explizit erwähnt wurden. Die Ausrichtung auf die Anforderungen der Kernprozesse, der Einsatz geeigneter und zeitgemäßer Applikationen und einer sicheren und kostenbewussten IT-Architektur, sowie standardisierte HW- und SW-Ausstattung sind Anzeichen dafür, dass diese Themen bedacht wurden.

Eine weitere wesentliche Anforderung an die Entwicklung einer IT-Sicherheitsstrategie ist die **Einführung einer Sicherheitsrichtlinie**, welche in Form des Organisationshandbuchs für Benutzer bereits existiert und auf die auch bereits in der IT-Strategie verwiesen wird.

Ferner decken sich eine Vielzahl der Prinzipen und Ziele der IT-Strategie mit denen einer Sicherheitsstrategie.
[Empfehlung] Trotzdem wäre es anzuraten, der IT-Strategie ein separates Unterkapitel zu widmen, welches sich mit der IT-Security auseinandersetzt und

explizit die wichtigsten Grundsätze einer IT-Sicherheitsstrategie beschreibt. Dadurch würde man der IT-Security automatisch ein höheres Maß an Bedeutung beimessen und sie als einen wesentlichen Eckpfeiler der IT-Strategie wahrnehmen.
Als Nachschlagewerk zur detaillierten Entwicklung einer Sicherheitsstrategie sei nochmals auf Kapitel 5 der österreichischen Sicherheitshandbuchs verwiesen.

[Empfehlung] Zusätzlich wäre in dem Unterkapitel der IT-Strategie der „via donau“ zu erwähnen, dass es ein Sicherheitskonzept gibt und auf Basis welcher Standards und Best Practices dieses beruht. Es sollte deutlicher hervor gehoben werden, dass die IT nicht nur zur Unterstützung der Kernprozesse dient, sondern auch Maßnahmen ergriffen werden, um diese adäquat zu schützen.

8.1.2 IST-Sicherheitsanalyse der via donau

Bei der IST-Sicherheitsanalyse werden grundsätzlich die IT-Infrastruktur, die Nutzer- und Anwenderumwelt (Organisationsaufbau, personelle Sicherheit, Richtlinien usw.), sowie physische und umgebungsbezogene Sicherheitsmaßnahmen analysiert. Außerdem wird eine IST-Aufnahme des Netzes und der Netzsicherheit getätigt und festgehalten, welche existierenden Sicherheitsstandards bisher im Einsatz waren. Bedrohungs- und Risikoanalysen führen zur Ermittlung von Bedrohungen und Verwundbarkeiten der gesamten Infrastruktur.

Eine vollständige IST-Sicherheitsanalyse kann in dieser Arbeit leider nicht durchgeführt werden, da dies zu umfangreich wäre. Jedoch soll aufgrund einer oberflächlichen Prüfung festgestellt werden, ob und wo möglicherweise Verbesserungspotential besteht.

Analyse der IT-Infrastruktur der via donau

- IT-Infrastruktur unterstützt ca. 240 Mitarbeiter

- Server an zwei Standorten in Wien (95 bzw. 70 Benutzer), vier kleinere Außenstellen (3-mal 15, sowie einmal 5 Benutzer) und einzelne Arbeitsplätze an den 9 Donauschleusen (verbunden durch eine IP-VPN Lösung zur Daten- und Sprachkommunikation)

- Wesentliche Benutzeranwendungen: MS-Office und Lotus Notes unter MS Windows XP, Personalmanagementsystem (für eine geringere Anzahl an Benutzern), ERP-System und spezifische GIS Anwendungen

- Serverseitige Anwendungen: File- und Printserver Windows 2003, Lotus Notes Domino Server, Web-Mail und Blackberry, Oracle Datenbanken für Personalmanagement- und ERP-System, sowie spezifische GIS Anwendungen. Die Benutzerdatenverwaltung erfolgt über Open LDAP, Backup über SEP Sesam und Virencheck über Ikarus.

- Die Anwendungen und Dienste werden überwiegend auf VMware virtualisierten Servern der Marke Dell (Poweredge Rack-Server) betrieben.

- Server- Betriebssysteme sind Linux und MS-Windows 2003

Analyse der Nutzer- und Anwenderumwelt

- Vorschriften für den Umgang zur Benutzung der Infrastruktur

- Sicherheitsrichtlinien zur Nutzung der IT-Infrastruktur (Organisationshandbuch für IT-Benutzer), insbesondere der Zugang zum Netzwerk. Darunter fallen die Passwortnutzung und die Nutzung des Netzwerks. Weiters vorhanden ist eine Richtlinie zur Internet-, Email- und Datennutzung

Analyse der physischen und umgebungsbezogenen Sicherheit

- Bauliche und infrastrukturelle Maßnahmen sind ausreichend vorhanden (z.B. Zugangskontrollen, Regelungen von Brandschutz, Stromversorgung, etc.)

Sonstige bereits getätigte Sicherheitsmaßnahmen (laut Organisationshandbuch des ZIT)

- Configuration-Management, Incident-Management, Problem-Management, Change-Management, Data- Management, Security-Management, Asset- und Lizenz-Management und das Disaster & Recovery Management

Durchführen einer Bedrohungs- bzw. Risikoanalyse

- wurde nicht durchgeführt, da dies den Umfang dieser Arbeit überschreiten würde

8.1.2.1 Empfehlungen zur IST-Sicherheitsanalyse der via donau

Bei der IST-Analyse ist aufgefallen, dass eine vollständige Aufstellung der Vermögenswerte der „via donau“ vorhanden und dokumentiert ist. Dabei wurde ein Abgleich mit den Empfehlungen aus Kapitel 7 „Vermögenswerte und Klassifizierung von Informationen“ des österreichischen Sicherheitshandbuch vorgenommen. Es liegen konkrete Listen bezüglich der zum Einsatz kommenden Vermögenswerte vor:

- **IT-Systeme** (inkl. eindeutiger Nummerierung, Beschreibung, Plattform, Aufstellungsort, Status, zuzuordnende Anwendungen, etc.)
- **Netzpläne** (inkl. IT-Systeme, aktive Netzkomponenten, Netzverbindungen, etc.)
- **Datenträger** (Archiv- und Backup-Datenträger, Externe Festplatten, USB-Sticks, Smartphones für den mobilen Einsatz, usw.)
- **Gebäude und Räume**

- **Anwendungen und Dienste**, die zum Einsatz kommen

Darüber hinaus gibt es zu den Vermögenswerten klar definierte Verantwortlichkeiten, welche im Organisationshandbuch des ZIT festgehalten sind.

[Empfehlung] Zusätzlich könnte man jedoch eine gruppierte Liste aller Vermögenswerte erstellen, in der eine Zuordnung der Verantwortlichkeiten genauestens geregelt ist.

[Empfehlung] Die Einführung von Sicherheitsklassen und die somit entstehende Kennzeichnung der Vermögenswerte bezüglich ihres Schutzbedarfs sind weitere eventuell zu tätigende Maßnahmen, die während der IST-Sicherheitsanalyse entdeckt wurden. Jede derart definierte Sicherheitsklasse gibt die Anforderungen bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit des Vermögenswerts wieder [BKÖ10].

Zu erwähnen sei aber, dass bezüglich der Verfügbarkeit der Vermögenswerte bereits ein Klassifizierungsschema bei der „via donau“ eingeführt wurde, welches man nun bei Bedarf um die Schutzwerte der Vertraulichkeit und Integrität erweitern könnte, zum Schutz der Informationen des Unternehmens (siehe dazu Kapitel 5.2.5 des österreichischen Sicherheitshandbuchs).

8.1.3 Auswahl von Bestandteilen aus existierenden Standards und Best Practices

In dieser Phase würde aufgrund der eventuell neu entdeckten Schwachstellen und Bedrohungen, welche im Rahmen einer IST-Sicherheitsanalyse aufgetreten sind, eine Auswahl von Bestandteilen aus existierenden Standards und Best Practices erfolgen, mit dem Ziel, die Schwachstellen zu beseitigen und diese in ein nachhaltiges Sicherheitskonzept einfließen zu lassen.

8.1.4 Entwurf des Sicherheitskonzepts der via donau

Untenstehend werden die Anforderungen auf taktischer Ebene aufgelistet, die zur Erfüllung eines nachhaltigen IT-Security Managementkonzept dienen. Die Aufzählung erfolgt im Abgleich mit den bereits getätigten Sicherheitsmaßnahmen der „via donau“. Sind konkrete Anforderungen nicht oder nur teilweise erfüllt, werden sie um Empfehlungen ergänzt.

- **Minimierung klassischer Risikofaktoren:** diese grundlegende Anforderung wurde bei der Erstellung der IT-Strategie berücksichtigt. Getätigte Maßnahmen sind sowohl im Organisationshandbuch für IT-Benutzer als auch im Organisationshandbuch für das ZIT und in weiteren Betriebshandbüchern beschrieben.

- **Einführung einer Sicherheitsrichtlinie:** wurde in der IT-Strategie als essentiell erfasst und im Unternehmen umgesetzt (siehe Kapitel 5 des Organisationshandbuchs für IT-Benutzer).

- **Einführung einer IT-Compliance:** zur Erfüllung von IT-Compliance Anforderungen wird auf den COBIT-Standard als Referenzmodell zurückgegriffen. Um die Vielzahl der regulatorischen und geschäftlichen Anforderungen zu erfüllen, gibt es beispielsweise ein internes Kontrollsystem, IT-Richtlinien, Regelungen zum Lizenz- und Asset-Management, Security-Management, Incident-Management etc.

  [Empfehlung] Eine eventuelle Verbesserung wäre, den Aspekt des Vorhandenseins einer IT-Compliance auch schriftlich zu dokumentieren. Beispielsweise in einem Kapitel, welches die wesentlichen Compliance-Anforderungen der „via donau“ umfasst, sowie getätigte Maßnahmen, um diese zu erfüllen.

- **Unabhängigkeit des Konzepts von der technologischen Ebene:** diese Anforderung wird in gewisser Weise auch berücksichtigt. Zwar gibt es kein konkretes IT-Security Managementkonzept, daher kann man auch nicht behaupten, dass das Konzept unabhängig von der

technologischen Ebene ist. Jedoch ist in der IT-Strategie verankert, dass eine standardisierte HW- und SW-Ausstattung für die Benutzer dazu führen soll, dass individuelle Anpassungen für spezifische Anforderungen auf ein Minimum reduziert werden.

- **Berücksichtigung neuer Technologien:** die Berücksichtigung neuer Technologien stellt für „via donau“ bisher keinen wesentlichen Aspekt dar. Man ist im Moment auf den Einsatz von standardisierter und zeitgemäßer Technologien für die Infrastruktur fokussiert – mit dem Ziel, eine hohe Verfügbarkeit, Ausfallsicherheit und IT-Sicherheit zu garantieren. Weiters präferiert die „via donau“ den Einsatz von erprobten und am Markt bewährten Standardapplikationen mit der Ausrichtung auf eine homogene Applikationslandschaft und Beseitigung bestehender Heterogenität in gewissen Teilbereichen.

  Dennoch gibt es einen Punkt in der IT-Strategie der sich mit dem Umgang von neuen Technologien (Innovationen) beschäftigt. Ziel ist es neue Technologien vorausschauend für den Einsatz bei der „via donau“ zu bewerten und im Bedarfsfall einzusetzen. Es wird dabei darauf geachtet als Innovator zu agieren, falls es dadurch zu Verbesserungen von Verfügbarkeit und Ausfallsicherheit kommt.

  [Empfehlung] Dies ist auf alle Fälle sehr zu begrüßen und sollte unbedingt auch weiterhin berücksichtigt werden, um eine zeitgemäße zukunftsorientierte IT-Sicherheit zu gewährleisten. Ergänzend sollte man auch Verbesserungen bezüglich der Integrität und Authentizität mit aufnehmen, da dies grundsätzliche Ziele der IT-Sicherheit sind.

- **Auslegung auf Prozesse und deren Veränderungen:** Die Ausrichtung auf die Anforderungen der Kernprozesse des Unternehmens und deren Veränderungen ist als ein wesentlicher Punkt in der IT-Strategie der „via donau“ festgehalten und wird auch so bei IT-Planungen und Umsetzungen gelebt.

- **Fähigkeit, auf Umstrukturierungen der IT reagieren zu können:** durch ein strukturiertes Change-Management und eine standardisierte HW- und SW-Ausstattung wird gewährleistet, dass auf Umstrukturierungen im IT-Bereich entsprechend reagiert werden kann und IT-Risiken minimiert werden.

- **Berücksichtigung neuer Bedrohungsszenarien:** Wie im bereits vorgestellten Prozess zur Einführung eines Security Managementkonzepts erwähnt, ist die Berücksichtigung neuer Bedrohungsszenarien ein wichtiger Punkt, den es auf taktischer Ebene eines Unternehmens umzusetzen gilt. Wünschenswert ist hierbei ein proaktives Handeln der Sicherheitsverantwortlichen. Es gilt die Entwicklung neuer Bedrohungsszenarien zu beobachten, um in weiterer Folge zeitgemäß und vor dem Eintreten dieser Maßnahmen zu setzen.

  Bei der „via donau“ sind dazu teilweise Maßnahmen getätigt worden, die zu einer Einschränkung neuer Bedrohungen führen sollen, beispielsweise durch automatische Virenupdates, regelmäßige Security-Checks durch externe Unternehmen, Einführung eines IDS etc.

  [Empfehlung] Um diese Anforderung bei der „via donau“ gänzlich zu erfüllen, sollte im Sicherheitskonzept (Kapitel des Security-Managements bei der „via donau“) verankert werden, dass sich Verantwortliche regelmäßig mit den Entwicklungen neuer Bedrohungsszenarien auseinandersetzen und anschließend überprüfen, inwiefern diese für das Unternehmen relevant sind. Dadurch kann nachhaltig die Qualität des Security-Managements gesteigert werden.

- **Berücksichtigung von Schwachstellen bezüglich der Protokollsicherheit:** **[Empfehlung]** Die zukünftige Weiterentwicklung des *S-BGP (Secure Border Gateway Protocol), TSIG (Transaction Signatures)* und *DNSSEC (DNS-Security)* ist zu beobachten und bei Ausgereiftheit umzusetzen. Bis dahin sollte dieser Sicherheitsaspekt

beim Eintreten von Sicherheitszwischenfällen als mögliche Ursache berücksichtigt werden.

8.1.5 Umsetzung des Sicherheitskonzepts (Betrieb)

Bei der Umsetzung des Sicherheitskonzepts wird anfangs überprüft, ob die Anforderungen der vorhergehenden Phasen an ein nachhaltiges Security Managementkonzept berücksichtigt wurden. Ist dies nicht der Fall, müssen von den Verantwortlichen entsprechende Maßnahmen und Nachbesserungen getätigt werden. Zusätzlich müssen auch in dieser Phase weitere Anforderungen umgesetzt werden, um die Vollständigkeit des Konzepts zu gewährleisten.

In diesem Kapitel wird nun überprüft, inwieweit die „via donau“ diese Anforderungen der operativen Ebene in seinem Unternehmen umgesetzt hat.

- **Kommunikation der Sicherheitsrichtlinien:** Die Kommunikation der Sicherheitsrichtlinie (Organisationshandbuch IT-Benutzer), sowie zusätzliche Benutzerdokumentation erfolgt über das Intranet der „via donau“. Die Formulierungen der Richtlinien sind entsprechend der Zielgruppe (IT Benutzer und internes IT Organisationshandbuch) klar verständlich und falls Unklarheiten vorherrschen, kann der Helpdesk kontaktiert werden.

  [Empfehlung] Jedoch wäre es sinnvoll hinzuzufügen, dass die Einhaltung der Richtlinien von großer Bedeutung für das Unternehmen ist sowie das Aufzeigen von Konsequenzen, die eine Nichteinhaltung mit sich bringen könnte. Darüber hinaus sollte jeder Mitarbeiter dazu angehalten werden, die Richtlinien zu lesen und diese zu befolgen. Dies gilt selbstverständlich auch für neu eintretende Mitarbeiter. Eine Aktualisierung der Richtlinien sollte ebenfalls allen Mitarbeitern zur Kenntnis gebracht werden.

- **Mitarbeiterschulungen und Awarenesstrainings:** Schulungen und Awarenesstrainings sind ebenfalls Maßnahmen, die angedacht werden

sollten. **[Empfehlung]** Dies sollte bei der „via donau“ in Abwägung des Kosten-Nutzen-Effekts getan werden. Trainings können eventuell auch auf Arbeitsgruppen eingegrenzt werden, die in einem besonderen Maß im Umgang mit IT-Security sensibilisiert werden sollten.

- **Nutzung von effizienten Authentifizierungstechnologien:** Die Nutzung effizienter Authentifizierungstechnologien ist wie bereits beschrieben eine wesentliche Anforderung, die es auf operativer Ebene umzusetzen gilt. Während der Durchsicht der IT-Strategie und den Unterlagen der „via donau“ wurde klar, dass dieser Anspruch in einem ausreichenden Maß erfüllt zu sein scheint. Es kommen sowohl auf Hardware- als auch auf Softwareebene entsprechende Lösungen, wie Verschlüsselungsverfahren, Protokolle, Zertifikate, Passwörter, Smartcards, etc. zum Einsatz.

- **Umsetzung eines funktionierenden und nachhaltigen Identitätsmanagement:** Die Umsetzung dieser Anforderung wird laut der IT-Strategie der „via donau“ angestrebt. Erklärtes Ziel ist es ein einheitliches und verbessertes Benutzermanagement aller Applikationen zu schaffen. Zukünftig will man den Benutzern zum einen Single-Sign-On-Funktionen bieten, anderseits soll auch die laufende Administration vereinfacht werden. **[Empfehlung]** Zusätzlich wäre es empfehlenswert, dem Identitätsmanagement ein eigenes Kapitel im Organisationshandbuch des ZIT zu widmen, sowie auch den Aspekt des Federated Identity Management einfließen zu lassen, welches sich mit der Identitätsbereitstellung und Verwendung über die Unternehmensgrenzen (Stichwort: zunehmende globale Vernetzung) hinweg beschäftigt.

  Die Umsetzung dieser Anforderung vereinfacht nicht nur die Administrierbarkeit und Pflege der Benutzerdaten, sondern bietet darüber hinaus einen größeren Schutz sensibler Informationen und hat damit auch einen enormen nachhaltigen Nutzen für das Unternehmen.

- **Einsatz sicherer Software:** Weiters gilt sicherzustellen, dass auf operativer Ebene nur sichere Software zum Einsatz kommt. Dies sollte bei der „via donau“ auf jeden Fall gewährleistet sein, da bereits in der IT-Strategie festgelegt wurde, dass man nur auf am Markt erprobte und bewährte Software und Applikationen zurückgreift.

- **Einführung von Monitoringmechanismen:** Bezüglich der Einführung von Monitoringmechanismen sind bereits Maßnahmen von der „via donau“ getätigt worden. Es gibt ein laufendes Monitoring (mittels Nagios), sowie eine präventive Wartung der IT-Infrastruktur, um die wichtigsten Bedrohungen zu minimieren. Insbesondere sind regelmäßige Security-Checks durch ein externes Unternehmen vorgesehen und sollen ebenfalls zur Überwachung und Verbesserung der IT-Security beitragen. Die Einhaltung der Sicherheitsrichtlinien wird stichprobenartig überprüft.

  [Empfehlung] Zu empfehlen ist, die Weiterentwicklung der derzeitigen Monitoringtools zu beobachten, da hier zukünftig ein Augenmerk auf die Schaffung von dynamischen Schutzmechanismen gelegt wird, welche sofort und automatisch auf Angriffe reagieren, sobald diese nachgewiesen werden. Sobald sich dieser Typus von Monitoringtools durchsetzt und bewährt hat, könnte man auch über Einführung bei der „via donau“ nachdenken, was eine weitere Verbesserung der IT-Security als Konsequenz hätte.

- **Umsetzung von Disaster Recovery- und Datenwiederherstellungsmaßnahmen:** Die Umsetzung eines Disaster & Recovery Management ist im Organisationshandbuch des ZIT der „via donau“ ausführlich beschrieben. Darüber hinaus wurde ein Maßnahmenplan festgelegt, wie die Datensicherung und -wiederherstellung garantiert werden kann.

8.1.6 Audits

Mittels regelmäßig durchgeführter Sicherheitsaudits werden die definierten Anforderungen und deren Umsetzungen bezüglich der IT-Security auf ihre Wirksamkeit im Unternehmen geprüft. Beispielsweise kann überprüft werden, ob die Vorschriften der IT-Compliance erfüllt sind, ob bestehende Maßnahmen zur Aufrechterhaltung des Sicherheitsniveaus nach wie vor geeignet sind, ob diese korrekt umgesetzt werden und auch von allen Beteiligten eingehalten werden. Die Durchführung sollte von der internen Revision oder externen Partnern erfolgen.

Bei der „via donau“ werden hinsichtlich der Qualitätssicherung folgende Maßnahmen getätigt, die zur Erhaltung des Sicherheitsniveaus beitragen:

- In regelmäßigen Abständen ist ein Security-Check durch ein externes Unternehmen vorgesehen [VW10-ZIT].

- Im Sinne einer Qualitätssicherung werden die Organisationshandbücher einmal jährlich (im vierten Quartal), sowie alle begleitenden Dokumente halbjährlich (im ersten und dritten Quartal) durch den Gruppenleiter und IT-Leiter einem Review auf Aktualität unterzogen [VW10-ZIT].

- Zur Vorbeugung bzw. Einschränkung von möglichen Folgeschäden eines Sicherheitsvorfalles werden die Logfiles auf den Servern und auf der Firewall in regelmäßigen Abständen auf Anomalien überprüft [VW10-ZIT].

- Zur laufenden Überprüfung der Funktionstauglichkeit der Konzeption der Notfallmaßnahmen erfolgt eine regelmäßige Durchführung von entsprechenden Tests und simulierten Notfällen [VW10-ZIT].

Soweit die getroffenen Maßnahmen zur Qualitätssicherung auch umgesetzt werden, sind diese in ihrem Umfang für die Bedürfnisse der „via donau“ als ausreichend zu betrachten.

8.2 Resümee der Überprüfung

Bei der Überprüfung auf Praxistauglichkeit des entworfenen IT-Security Managementkonzepts stellte sich heraus, dass die Anwendbarkeit auf ein Unternehmen mittlerer Größe, wie es die „via donau“ ist, zufriedenstellend gegeben ist. Betont werden muss, dass nicht versucht wurde, das Konzept als neue Grundlage für IT-Security im Unternehmen zu integrieren. Es wurde jedoch schrittweise geprüft, ob bei Anwendung des Konzepts auf die „via donau“ bestehende und getätigte IT-Security Maßnahmen im Einklang mit den Anforderungen des entwickelten IT-Security Managementkonzepts sind. Dazu wurden die einzelnen Phasen des Prozesses zur Einführung des nachhaltigen IT-Security Managementkonzepts durchgegangen.

Bei der Phase „Festlegen der Sicherheitsstrategie“ stellte sich heraus, dass es keine gesonderte Sicherheitsstrategie für das Unternehmen gibt, obwohl die grundsätzlichen Anforderungen an die IT-Security in der IT-Strategie verankert waren. Daraus ergab sich die Empfehlung, die IT-Security stärker hervorzuheben und ihr ein eigenes Kapitel zu widmen. Zusätzlich fehlte in der IT-Strategie Information darüber, dass ein IT-Sicherheitskonzept im Unternehmen vorhanden ist, Sicherheitsmaßnahmen getroffen werden und auf welchen Standards und Best Practices diese basieren. Die Einführung einer gesonderten Sicherheitsstrategie wie im Konzept vorgesehen, hätte sich genau diesen Aspekten gewidmet. Zusätzlich hätte bei Vorhandensein einer Sicherheitsstrategie wie im Konzept grundsätzlich vorgesehen, einfach und schnell auf relevante Kapitel aus existierenden Planungsansätzen zurück gegriffen werden können.

In der Phase der „IST-Sicherheitsanalyse“ wurden grundsätzlich die IT-Infrastruktur, Nutzer- und Anwenderumwelt sowie physische

Sicherheitsmaßnahmen analysiert. Bedrohungs- und Risikoanalysen wurden aufgrund des zusätzlichen Mehraufwands nicht durchgeführt. Die Empfehlungen, welche sich daraus ergaben, ließen sich aus den entsprechenden Kapiteln des österreichischen Sicherheitshandbuchs ableiten. Stattdessen bzw. ergänzend hätte auch der BSI- oder ISO-Standard hinzugezogen werden können.

In der darauf folgenden Phase „Auswahl von Bestandteilen aus existierenden Standards und Best Practices“ hätte bei Bedarf versucht werden können, die entdeckten Schwachstellen und Bedrohungen, welche im Rahmen einer IST-Sicherheitsanalyse aufgetreten sind, durch Auswahl von Bestandteilen aus existierenden Standards und Best Practices zu beseitigen.

In der Phase „Entwurf des Sicherheitskonzepts“ erfolgte eine Überprüfung, ob die Anforderungen an die IT-Security auf taktischer Ebene bei der „via donau“ umgesetzt wurden. Dabei stellte sich heraus, dass prinzipiell alle Anforderungen erfüllt waren, dies aber nicht auf Anhieb festgestellt werden konnte. Zurück zu führen ist dieser Umstand darauf, dass es kein dokumentiertes Sicherheitskonzept bei der „via donau“ gibt. Die Informationen bezüglich der getätigten Maßnahmen zur Erfüllung der Anforderungen an die IT-Security sind auf verschiedene Dokumente (IT-Strategie, Organisationshandbuch für IT-Benutzer, Organisationshandbuch des ZIT) verteilt. Das Vorhandensein eines dokumentierten und strukturierten Sicherheitskonzepts, wie grundsätzlich gefordert, würde langfristig und nachhaltig zur Verbesserung der IT-Security beitragen. Anpassungen und Veränderungen am Sicherheitskonzept wären leichter zu tätigen, sowie die Auswirkungen auf die verschiedenen Bereiche des Unternehmens besser nachzuvollziehen.

In der Phase „Umsetzung des Sicherheitskonzepts (Betrieb)“ wurde ein Abgleich der notwendigen operativ zu tätigenden Anforderungen für ein nachhaltiges IT-Security Managementkonzept, mit den getätigten Maßnahmen der „via donau“ durchgeführt. Wie erhofft, waren beispielsweise die

Sicherheitsrichtlinien und deren Formulierung entsprechend der Zielgruppen definiert und den Mitarbeitern auch kommuniziert. Allerdings stellte sich heraus, dass gegenüber den Mitarbeitern zu wenig hervorgehoben wird, welch schwerwiegende Konsequenz eine Nichteinhaltung der Sicherheitsrichtlinie für die IT-Security, aber auch für das gesamte Unternehmen haben kann. Maßnahmen wie Mitarbeiterschulungen und Awarenesstrainings werden zudem wie in vielen anderen Unternehmen vernachlässigt, obwohl sie enorm positive Auswirkungen für Unternehmen haben könnten. Die im Konzept geforderte Anforderung zur Einführung von Monitoringtools wird bei der „via donau“ bereits umgesetzt. Ferner wurde aber auch explizit darauf hingewiesen, dass es hier demnächst bzw. in naher Zukunft zu Weiterentwicklungen kommen wird, die zu einer nachhaltigen Verbesserung der IT-Security beitragen können.

Zum Abschluss wurde überprüft ob regelmäßig durchgeführte Sicherheitsaudits in der Sicherheitsphilosophie des Unternehmens erwägt und durchgeführt werden. Hierbei stellte sich heraus, dass diese in ihrem derzeitigen Umfang zur Erfüllung eines nachhaltigen Security Managementkonzepts beitragen würden.

Grundsätzlich kann behauptet werden, dass die Einführung bzw. Anwendung des nachhaltigen IT-Security Managementkonzepts bei der „via donau“ zur Verbesserung des Sicherheitsniveaus beitragen könnte. Es zeigte sich, dass die in dieser Arbeit individuell definierten Anforderungen an ein nachhaltiges IT-Security Management in Kombination mit den bestehenden Vorgehensweisen und Maßnahmen aus existierenden Planungsansätzen und Best Practices einen zusätzlichen positiven Output für IT-Security des Unternehmens generierten.

Die Empfehlungen, welche für die „via donau“ getroffen wurden, setzten sich einerseits aus Vorschlägen und Maßnahmen der existierenden Planungsansätze zusammen, andrerseits aus den individuellen Anforderungen des IT-Security Managementkonzepts. Jene Empfehlungen, die sich aus den Anforderungen ableiten ließen, leisten einen wertvollen Beitrag zur Nachhaltigkeit und zukünftigen Verbesserung des Sicherheitsniveaus. Es wurde

zudem auf aus heutiger Sicht nicht vollkommen beseitigte Schwächen in der IT-Security Branche (Protokollsicherheit, Bedrohungsszenarien, etc.) hingewiesen, die Anlass für Sicherheitszwischenfälle sein können. Ferner konnte für die „via donau“ aufgezeigt werden, in welchen Bereichen der IT-Security (Monitoringmechanismen, Identitätsmanagement, etc.) es in absehbarer Zeit zu Weiterentwicklungen kommen kann und auch wird.

Zusammenfassend lässt sich urteilen, dass die „via donau“ eine Vielzahl von grundsätzlichen Anforderungen der IT-Security berücksichtigt hatte, diese aber nicht konkret in Zusammenhang mit dem Thema gebracht worden sind. Des Weiteren waren die getätigten und die noch in Zukunft zu tätigenden Maßnahmen über diverse Dokumente verteilt. Das Vorhandensein eines nachhaltigen IT-Security Managementkonzepts, welches eine konkrete IT-Sicherheitsstrategie und ein IT-Sicherheitskonzept umfasst, würde genau diese Schwächen beseitigen, einen Gesamtüberblick über die IT-Security Lage der „via donau“ geben und in Folge dessen einen wertvollen Beitrag zur Verbesserung der Security für das Unternehmen leisten.

9 Ausblick auf weitere Forschungstätigkeiten

Zur Umsetzung dieser Arbeit wurden diverse Empfehlungen und wissenschaftliche Ansätze aus der Literatur in das IT-Security Managementkonzept eingearbeitet. Die zentrale Fragestellung in diesem Kapitel beschäftigt sich nun mit der Beurteilung, inwiefern es gelungen ist, die Vorschläge zu berücksichtigen. Es soll darauf hingewiesen werden, welche wissenschaftlichen Ansätze und Empfehlungen im Konzept konkret umsetzbar waren, aber auch was aus heutiger Sicht praktisch noch nicht vollständig realisierbar ist bzw. in welchen Bereichen aus persönlicher Wahrnehmung noch Forschungsarbeit geleistet werden muss.

9.1 Authentifizierungstechnologien

Authentifizierungstechnologien, wie in [NCO05] beschrieben, dienen als wesentlicher Bestandteil von vernetzten Einheiten und werden darüber hinaus für eine Vielzahl von Verwendungszwecken eingesetzt. Wie jedoch bereits in Kapitel 5.1 erwähnt, besteht die Schwäche der Authentifizierung darin, dass traditionelle Methoden der Kryptographie nicht auf diese großflächige Verbreitung und Nutzung über das Internet ausgelegt waren. Daher wurde auch von [NCO05] empfohlen, weitere Anstrengungen in die Forschung hinsichtlich Infrastruktur und Protokolle für „Large-Scale Key Distribution and Management“ zu betreiben, um in diesem Gebiet Verbesserungen zu erreichen.

Aus der Perspektive der KMUs für die das IT-Security Managementkonzept ausgelegt ist, gilt es in Hinsicht auf die Authentifizierungstechnologien abzuwägen, welche der vielen derzeit zur Verfügung stehenden Verfahren (z.B. diverse Verschlüsselungsverfahren, Protokolle, Zertifikate, etc.) oder auf Benutzerebene (Passwörter, Smartcards, Biometrielösungen, etc.) für ihre Unternehmen am besten geeignet sind. Wenn möglich, sollte bei den Lösungen auf offene Standards gesetzt werden, die eine Vielzahl von Komponenten unterstützen. Des Weiteren gilt, dass die zum Einsatz kommenden

Technologien auf vorhandene Anwendungs- und Netzinfrastrukturkomponenten aufbauen sollten, ohne dass zusätzliche Hard- und Software erforderlich ist.

Zusammenfassend würde es sich für IT-Security Verantwortliche empfehlen, grundlegende Entwicklungen dieses Themengebiets weiterhin zu beobachten und bei Bedarf und Ausgereiftheit von beispielsweise neuen Protokollen, Zertifikaten, etc., diese in ihre Unternehmen zu integrieren. Abschließend muss auch nochmals erwähnt werden, dass die große Bedeutung von Authentifizierungstechnologien für diese Arbeit darin liegt, dass sie grundlegend zur IT-Security beitragen und im engen Konnex zu anderen wesentlichen Anforderungen des IT-Security Managementkonzepts, wie Identitätsmanagement und Cloud Computing stehen.

9.2 Protokollsicherheit

Als ein weiterer kritischer Faktor bezüglich der Security wurde in [NCO05] die Protokollsicherheit im Internet erwähnt. Speziell hervorgehoben wurden dabei der einfache Missbrauch des „Border Gateway Protocol (BGP)“ und des Domain Name System (DNS) Service. Die Autoren des [NCO05] plädieren für die Entwicklungen von sicheren Protokollen zur Vermeidung von DoS-Attacken, um die Beschädigung und Verfälschung von Informationen zu vermeiden und das Internet somit zu einem verlässlicheren Kommunikationsmedium zu machen. In Anbetracht der zunehmenden Vernetzung von Unternehmen über das Internet und des ständig ansteigenden Einflusses des Cloud Computings gilt es hierfür eventuelle Weiterentwicklungen zu beobachten. Ein interessanter Ansatz zur Verbesserung des BGPs wurde in [KLS00] beschrieben. Es scheint jedoch, dass sich das dort beschriebene „Secure Border Gateway Protocol“ (S-BGP) trotz seiner theoretisch beschrieben Vorteile gegenüber des herkömmlichen BGPs in der Praxis bisher nicht durchsetzen konnte und kann. Bis es auf diesem Gebiet zu Verbesserungen kommt, sollte stets in Erwägung gezogen werden, dass Sicherheitszwischenfälle auf Schwächen des BGP zurückzuführen sein könnten.

Die hingegen ebenfalls in dieser Arbeit bereits erwähnten Erweiterungen des DNS-Protokolls, wie DNSSEC (DNS-Security) und TSIG (Transaction Signatures) finden in der Praxis bereits ihren Einsatz. Hinzugefügt werden muss aber trotzdem, dass auch hier kritische Stimmen vorhanden sind, welche auf Schwachstellen und Praxis-Probleme hinweisen. Dies lässt darauf schließen, dass es auch in Zukunft zu Veränderungen und Entwicklungen bei der Protokollsicherheit kommen wird, welche man aber aus heutiger Sicht noch nicht genau voraussehen kann. Für Unternehmen sollte bis dahin gelten, DNSSEC (DNS-Security) und TSIG (Transaction Signatures) als einen wesentlichen Baustein bzw. Maßnahme zur Verbesserung der IT-Security in ihr Konzept aufzunehmen.

9.3 Identitätsmanagement

In dieser Arbeit wurde ebenfalls Bezug auf das Identitätsmanagement genommen, welches in Zukunft zunehmend eine zentrale Rolle zum Schutz sensibler Daten eines Unternehmens darstellen wird. Verstärkt wird diese Annahme durch Trends wie Cloud Computing oder IT-Consumerization und daraus resultierend den Umgang mit Identitäten über Unternehmensgrenzen hinweg. In [CSA10] und [SM09] werden die grundlegenden Identity- und Access Managementmethoden für ein erfolgreiches und effektives Management von Identitäten in der Cloud diskutiert. Speziell wird dabei auch näher auf das in dieser Arbeit bereits erwähnte Federated Identity Management eingegangen. Weiters werden in [CSA10] speziell die Anforderungen, Herausforderungen zur Umsetzung eines Federated Identity Management näher beschrieben. Darüber hinaus werden Lösungen und Empfehlungen zur Umsetzung eines selbigen zur Verfügung gestellt.

Über kurz oder lang wird es für Unternehmen, welche ihr Identitätsmanagement planen oder versuchen zu verbessern, unvermeidbar, den Aspekt des Federated Identity Management zu berücksichtigen. Bei der Umsetzung des in dieser Arbeit vorgestellten IT-Security Managementkonzept sollte unbedingt über Funktionen nachgedacht werden, welche die Identitätsbereitstellung und -

verwendung über die Unternehmensgrenzen hinweg ermöglichen, um spätere Anpassungen zu vermeiden und eine gewisse Nachhaltigkeit zu gewährleisten.

9.4 Monitoring – dynamische Schutzmechanismen

Da wie bereits in dieser Arbeit festgestellt wurde, eine hundertprozentige Sicherheit nicht garantiert werden kann, gilt es zumindest als unerlässlich, die IT-Infrastruktur zu monitoren, um irreguläre Netzwerkaktivitäten aufzuzeigen und Sicherheitszwischenfälle zu reduzieren. In [NCO05] wird darauf hingewiesen, dass gegenwärtige Monitoringtools in ihrer Funktion zu primitiv seien. Es besteht der Bedarf nach dynamischen Schutzmechanismen, welche selbstständig reagieren und agieren, wenn Angriffe auf Systeme identifiziert wurden. Ein weiteres interessantes Forschungsfeld zu diesem Themengebiet wäre beispielsweise das Entwickeln von Monitoringmechanismen, welche automatisch überprüfen, ob die IT-Systeme den vorgegebenen Richtlinien eines Unternehmens entsprechen.

Der Aspekt des Monitorings, sowie die Berücksichtigung von dynamischen Schutzmechanismen wurden im IT-Security Managementkonzept dieser Arbeit als wesentliche Anforderung hinzugefügt, da hier laut [NCO05] zukünftig enormes Potential für Unternehmen gesehen wird. Dies erfolgte, obwohl speziell die dynamischen Schutzmechanismen in ihrer derzeitigen Form noch nicht in der Praxis umsetzbar sind. Bis auf weiteres sollte unbedingt auf bewährte Monitoringtools zurückgegriffen werden, bis es auf diesem Gebiet zu Weiterentwicklungen kommt, die dann in der Praxis verwendet werden können.

9.5 Automatisierung der Information Security

Das Kapitel 4.5.1 dieser Arbeit setzte sich bereits mit dem Thema der Information Security Automatisierung näher auseinander. Die dabei erwähnten Autoren stellten in [FM11] fest, dass die Umsetzung eines ISMS anhand existierender Planungsansätze, wie es der ISO 27001 Standard ist, einen wertvollen Beitrag zur Gestaltung der IT-Security leistet. Jedoch wurde dabei auch offenkundig, dass die Umsetzung sehr aufwendig und umfangreich ist,

speziell wenn man eine Compliance bezüglich des Standards erreichen will. Es wird die Berücksichtigung einer Vielzahl von Kontrollzielen bzw. Maßnahmen (mehr als 130) gefordert, um konform mit den Anforderungen des ISO-Standards zu sein. Dies wiederum kann speziell KMUs vor größere Probleme stellen. Sei es zum einen, dass für diese Aufgaben zu wenig Personal vorhanden ist, es zu wenig geschulte Mitarbeiter gibt, oder der zu tätigende Zeitaufwand nicht dem Kosten-Nutzen-Effekt des Unternehmens entspricht.

Bei der Untersuchung in [FM11] stellte sich weiters heraus, dass derzeit in etwa nur ca. 28% der zu tätigenden Maßnahmen des ISO 27001 Standards automatisiert abgearbeitet werden können. Dazu wären den Schlussfolgerungen der Autoren in [FM11] zu Folge mehrere unterschiedliche Tools von diversen Herstellern nötig. Aus der Perspektive von KMUs wird sich die Anschaffung dieser Tools daher nicht lohnen, da im Moment nicht abgeschätzt werden kann, inwiefern die Tools für den täglichen Unternehmensalltag ausgereift sind und ob diese auch wirklich kompatibel zueinander sind.

In diesem Zusammenhang sei jedoch nochmals auf das in dieser Arbeit erwähnte Security Content Automation Protocol (SCAP), auf welches in [FM11-1] und im Kapitel 4.5.2 näher eingegangen wurde, erwähnt, welches sich mit der Problematik zur Schaffung von mehr Interoperabilität zwischen Security-Tools auseinandersetzt. Dabei handelt es sich um eine Initiative von mehreren Organisationen, welche bemüht sind, dieses Mehrzweckprotokoll weiterzuentwickeln, um einen Standard zu schaffen, der sich in absehbarer Zukunft durchsetzen wird. Es gibt Kennzeichen dafür, dass dies auch gelingt, da immer mehr renommierte Sicherheitsmanagementlösungsanbieter das Security Content Automation Protocol in ihren Produkten berücksichtigen und nutzen.

Ein höherer Grad an Automatisierung hinsichtlich der Information Security und im speziellen der existieren Planungsansätze, wie dem ISO 27001 Standard, wäre auch für das in dieser Arbeit entworfene IT-Security Managementkonzept

von Vorteil, da dieses zu einem nicht unerheblichen Teil existierende Planungsansätze und Best Practices mit einbezieht. Wünschenswert wäre es, ein Tool zu besitzen, welches beispielsweise all die gegenwärtig automatisierbaren Kontrollziele bzw. Maßnahmen des ISO 27001-Standards abdecken würde. Im nächsten Schritt könnten anschließend Überlegungen getätigt werden, inwiefern auch andere Planungsansätze und Best Practices automatisierbar sind und ob ein einziges Tool das ganze Spektrum abdecken könnte. Oftmals erlangt man derzeit den Eindruck, dass speziell die Einarbeitung in die mehrere hundert Seiten umfassenden existierenden Planungsansätze, wie der ISO 27001-Standard oder das Grundschutzhandbuchs des BSI es sind, speziell für viele KMUs eine unüberwindbare Hürde darstellen.

Zusammenfassend kann durchaus behauptet werden, dass eine zunehmende Automatisierung der Information Security einen direkten Mehrwert für KMUs hätte, da mit geringeren Kosten und einer zeiteffizienteren Umsetzung von IT-Security Maßnahmen zu rechnen wäre. Die hohen Kosten und der immense Zeitaufwand waren bisher genau jene Aspekte, warum oftmals von Investitionen in die IT-Security abgesehen wurde und somit reduziert werden könnten.

10 Zusammenfassung und Ausblick

Die Masterarbeit hatte zum Ziel, ein nachhaltiges IT-Security Managementkonzept für kleine und mittlere Unternehmen zu entwerfen, welches zu einer Verbesserung bzw. nachhaltigen Steigerung des Sicherheitsniveaus beiträgt. Der Einsatz von Informations- und Kommunikationstechnologie ist aus dem normalen Unternehmensalltag nicht mehr wegzudenken; sie ist gewissermaßen der notwendige Schlüssel, um die Wettbewerbsfähigkeit einer Vielzahl von Unternehmen zu gewährleisten. Daher gilt es, die zum Teil sehr komplexen IT-Systeme auch adäquat zu schützen, was sich aber oftmals als nicht so einfach darstellt. Unternehmen sehen sich heutzutage bezüglich der IT-Security mit weitreichenden und ständig ändernden Herausforderungen konfrontiert, die von ihnen berücksichtigt werden sollten. Dazu zählen beispielsweise neben den technischen auch organisatorische und soziale Aspekte, die es zu berücksichtigen gilt. Den Überblick über aktuelle Entwicklungen in diesem Bereich zu bewahren, kann speziell für kleinere und mittlere Unternehmen äußerst schwierig sein.

Das in dieser Arbeit entwickelte IT-Security Managementkonzept, sowie die Vorgehensweise zur Einführung desselbigen soll genau jene Unternehmen unterstützen, die eine nachhaltige Verbesserung bezüglich ihrer IT-Security erreichen wollen. Dabei wurde versucht, auf aktuelle und zukünftige Herausforderungen der IT-Security auf allen Unternehmensebenen Rücksicht zu nehmen, sowie existierende Planungsansätze und Best Practices mit einzubeziehen, um so ein umfassendes den heutigen Sicherheitsanforderungen entsprechendes Konzept zur Verfügung zu stellen.

Anhand des Kapitels 8 wurde die Praxistauglichkeit des Konzepts auf die Anwendbarkeit bei der „via donau“, einem mittelständischen österreichischen Unternehmen, überprüft. Es stellte sich heraus, dass das Konzept prinzipiell gut auf Unternehmen mittlerer Größe anwendbar wäre. Im konkreten Fall der „via donau“ wurde überprüft ob bei Umlegung des Konzepts bestehende und

getätigte IT-Security Maßnahmen im Einklang mit den Anforderungen des entwickelten IT-Security Managementkonzepts sind. Zudem wurde ersichtlich, dass das entworfene IT-Security Managementkonzept dazu führt, Verbesserungspotentiale aufzuzeigen und somit seinen Zweck erfüllt. Aufgrund der Berücksichtigung der Prämisse der Nachhaltigkeit, sowie den dazugehörigen identifizierten Anforderungen und die Integration des PDCA-Zyklus in das Konzept sollten Unternehmen für zukünftige Entwicklungen der IT-Security der nächsten Jahre gerüstet sein. Darüber hinaus ergibt sich dadurch zusätzlich eine Minimierung der klassischen Risikofaktoren, da etwaige Sicherheitsmängel vermieden oder rasch identifiziert und behoben werden können. Dies kann in weiterer Folge beispielsweise positive Auswirkungen auf die Reputation eines Unternehmens haben, aber natürlich auch auf finanzielle Aspekte.

Grundsätzlich kann behauptet werden, dass das Konzept von einer Vielzahl von Unternehmen verwendet bzw. als Grundlage für das IT-Security Management herangezogen werden könnte, da es sich unter anderem auch auf existierende IT-Security Planungsansätze stützt. Für Großunternehmen hingegen ist der Einsatz des in dieser Arbeit aufgezeigten Ansatzes zur Einführung eines nachhaltigen IT-Security Managementkonzepts wahrscheinlich nur bedingt geeignet, da hierbei eine noch detailliertere Herangehensweise und eine noch größere Anzahl von Anforderungen an die IT-Security, die es zu berücksichtigen gilt, vorausgesetzt werden muss.

Zusammenfassend lässt sich sagen, dass das Thema der IT-Security ein sehr weitflächiges und teilweise sehr komplexes Gebiet ist, bei dem eine Vielzahl von Faktoren berücksichtigt werden müssen. Dazu zählen unter anderem wie bereits genannt technologische, organisatorische, soziale und rechtliche Aspekte, aber natürlich auch wirtschaftliche Aspekte. Als Schlagwort hierfür sei nochmals der Kosten-Nutzen-Effekt für ein Unternehmen erwähnt, welches in den Bereich der IT-Security investieren will. Um zum einen diesen Kosten-Nutzen-Effekt für Unternehmen zu optimieren, zum anderen natürlich um die IT-

Security noch effizienter zu machen, wird aus wissenschaftlicher Sicht daran gearbeitet, eine zunehmende Automatisierung der Information Security voran zu treiben. Ein weiteres wissenschaftliches Forschungsfeld beschäftigt sich mit der Schaffung von größerer Interoperabilität zwischen Sicherheitslösungen der unterschiedlichen Anbieter untereinander. In diesem Kontext setzt sich in letzter Zeit zunehmend das Security Content Automation Protocol (SCAP) durch.

Zum Schluss lässt sich festhalten, dass speziell der Bereich der IT-Security in Zukunft zunehmend eine zentrale Rolle in Unternehmen einnehmen wird und soll, da nahezu jeder Prozess eines Unternehmens in irgendeiner Form von IT-Systemen abhängig ist, die sensible Informationen verarbeiten, verwalten, speichern oder weiterleiten. Diese gilt es unbedingt entsprechend zu schützen und dies kann nur durch den Einsatz von entsprechenden IT-Security Managementkonzepten gewährleistet werden. Jedoch gilt es für Unternehmen auch als unerlässlich, neue Entwicklungen im Bereich der IT-Security weiterhin zu beobachten.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[AL11] Fernando Almeida, Justino Lourenco. ***Security Issues in Unified Communications.*** International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 2, April 2011

[And80] James P. Anderson. ***Computer Security Threat Monitoring and Surveillance.*** **Fort Washington,** PA, 1980

[BBZBJ10] Dr.Rainer Bernnat, Marcus Bauer, Dr. Wolfgang Zink, Dr. Nicolai Bieber, Dietmar Jost. ***Die IT-Sicherheitsbranche in Deutschland – Aktuelle Lage und ordnungspolitische Handlungsempfehlungen.*** Februar 2010 http://www.bmwi.de/BMWi/Navigation/Service/publikationen,did=333348.html [Stand: 16.5.2011]

[Ber10] Berlecon Research. ***Betriebsmodelle für Unified Communications im Mittelstand.*** Whitepaper. Mai 2010 http://www.berlecon.de/studien/downloads/Berlecon_WhitepaperUC_Avaya.pdf [Stand: 27.4.2011]

[Bis03] Matt Bishop**.** ***Computer Security, Art and Science.*** 4. Auflage, Pearson Education, Inc. 2003

[BKÖ10] Bundeskanzleramt Österreich. ***Österreichisches Informationssicherheitshandbuch.*** Version 3.1.000. 22.11.2010 https://www.sicherheitshandbuch.gv.at/ [Stand:25.8.2011]

[BÖ05] Dr. Wolfgang Böhmer. ***Auf der sicheren Seite – Informationssicherheitsmanagement und IT-Governance.*** Fachbeitrag – Risknews. Mai 2005 http://onlinelibrary.wiley.com/doi/10.1002/risk.200590090/abstract [Stand:29.5.2011]

[BOU10] Mark Bouchard. ***Network Security for 2010 and Beyond – The Impact of the Conumerization, Webification, Virtualization and Consolidation of IT.*** AimPoint Group. 2010 http://www.sonicwall.com/emea/569_15491.html [Stand: 17.5.2011]

[Bre07] Brennecke & Partner Rechtsanwälte. IT Sicherheit Teil 12/1 Zertifizierungen ISO. März 2007. http://www.brennecke-partner.de/87390/IT-Sicherheit-Teil-12-1-Zertifizierungen-ISO [Stand: 27.2.2011]

[BSI] Bundesamt für Sicherheit in der Informationstechnik (BSI). ***Zertifizierung.***

https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/zertifizierungnachccunditsec_node.html [Stand: 20.4.2011]

[BSI05] Bundesamt für Sicherheit in der Informationstechnik**.** ***ITIL und Informationssicherheit: Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management.*** *2005* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITIL/itil_pdf.pdf?__blob=publicationFile [Stand:29.5.2011]

[BSI09] Bundesamt für Sicherheit in der Informationstechnik*.* ***IT-Grundschutz-Kataloge – 11.Ergänzerungslieferung.*** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile [Stand: 20.3.2011]

[BSI10] Bundesamt für Sicherheit in der Informationstechnik**.** ***IT-Grundschutz-Profil für den Mittelstand – Version 2010*****.** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/it-grundschutz_profil_mittel.pdf?__blob=publicationFile [Stand: 22.3.2011]

[CA04] Richard A. Caralli. ***Managing for Enterprise Security.*** Networked Systems Survivability Program – Technical Note. December 2004. www.cert.org/archive/pdf/**managing**es0412.pdf [Stand: 7.6.2011]

[CC-1-09] The Common Criteria. ***Common Criteria for Information Technology Security Evaluation – Part1: Introduction and general model.*** Version 3.1. July 2009. http://www.commoncriteriaportal.org/supporting/ [Stand: 19.4.2011]

[CC-2-07] The Common Criteria. ***Common Criteria for Information Technology Security Evaluation – Part2: Security functional components.*** Version 3.1. September 2007. http://www.commoncriteriaportal.org/supporting/ [Stand: 19.4.2011]

[CC-3-09] The Common Criteria. ***Common Criteria for Information Technology Security Evaluation – Part3: Security assurance components.*** Version 3.1. July 2009. http://www.commoncriteriaportal.org/supporting/ [Stand: 19.4.2011]

[CEM09] The Common Criteria. ***Common Methodology for Information technology Security Evaluation.*** Version 3.1. July 2009. http://www.commoncriteriaportal.org/supporting/ [Stand: 20.4.2011]

[CSA10] Cloud Security Alliance. ***Domain 12: Guidance for Identity & Access Management V2.1.*** Version 2.1. 2010. http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf [Stand: 25.5.2011]

[FKLP08] Steven Furnell, Sokrates Katsikas, Javier Lopez, Ahmed Patel***. Securing Information and Communication Systems.*** Artech House, Inc. 2008.

[FM11] Stefan Fenz, Rayel Montesino. ***Information security automation: how far can we go?*** Sixth International Conference on Availability, Reliability and Security 2011.

[FM11-1] Stefan Fenz, Rayel Montesino. ***Automation possibilities in information security management.*** Proceedings of the European Intelligence and Security Informatics Conference 2011. September 2011

[FUR02] Furnell, S.M. ***Categorising Cybercrime and Cybercriminals: The Problems and Potential Approaches***. Journal of Information Warfare, Vol. 1, No. 2, 2002, pp. 35-44

[ISO08] International Standard Organization. ***Informationstechnologie - Sicherheitstechnik – Leitfaden für das Management der Informationssicherheit (ISO/IEC 27002:2005).*** August 2008.

[ISO10] International Standard Organization. ***Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2009).*** Mai 2010

[IT10-ORG] IT-Team***. IT-Organisationshandbuch für Benutzer.*** Version 1.1. März 2010

[Kau09] Lori M. Kaufman. ***Data Security in the World of Cloud Computing***. *IEEE Security and Privacy*, vol. 7, no. 4, pp. 61-64, July/Aug. 2009.

[KK08] Heinrich Kersten, Gerhard Klett. ***Der IT Security Manager.*** 2.Auflage, Vieweg+Teubner, 2008

[KLS00] Stephen Kent, Charles Lynn, Karen Seo. ***Secure Border Gateway Protocol (S-BGP).*** IEEE Journal on selected Areas in Communications, VOL. 18, NO. 4, APRIL 2000 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.1665&rep=rep1&t

ype=pdf [Stand: 23.5.2011]

[KP10] Dr.Kraus und Partner. ***Knowledgebase.*** http://www.kraus-und-partner.de/1414/Skalierbarkeit

[KRS09] Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder. ***IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz.*** 2.Auflage, Vieweg+Teubner, 2009

[KRA04] Thomas Krauß. ***Viren, Würmer und Trojaner.*** 1. Auflage, Weka Media GmbH & Co. KG

[LMMM00] Antonio Lioy, Fabio Maino, Marius Marian, Daniele Mazzocchi. ***DNS Security.*** Terena Networking Conference, May 22-25, 2000 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4154&rep=rep1&type=pdf [Stand: 23.5.2011]

[MA09] R.A. Martin. ***Making security measurable and manageable.*** *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2009, p. 1–9.

[NCO05] National Coordination Office for Information Technology Research and Development. ***Cyber Security: A Crisis of Prioritization.*** February 2005.

[QSBJ11] Stephen Quinn, Karen Scarfone, Matthew Barrett, Chris Johnsen. ***Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0.*** Recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-117. http://csrc.nist.gov/publications/nistpubs/800-117/sp800-117.pdf

[OVPC11] Office of the Victorian Privacy Commissioner. ***Information Sheet: Cloud Computing.*** May 2011

[PFL00] Charles P. Pfleeger. ***Security in Computing.*** 2.Auflage, Prentice Hall PTR, 2000

[Pie10] Jens Pientak. ***5 Praxisschritte zu einer nachhaltigen IT.*** http://www.cio.de/strategien/methoden/2226210/index2.html [Stand: 18.4.2011]

[Qui09] Gerald Quirchmayr. ***Secure Electronic Commerce.*** Vorlesungsunterlagen an der Universität Wien. Sommersemester 2009

[RB09] Matthias Riebisch, Stephan Bode. ***Software-Evolvability.*** Springer-Verlag 2009. http://www.theoinf.tu-ilmenau.de/~riebisch/home/publ/riebischbode_software-evolvability.pdf [Stand:

18.4.2011]

[Rich08] Robert Richardson, CSI Director**.** ***CSI Computer Crime & Security Survey****.* http://www.gocsi.com/forms/csi_survey.jhtml Stand: 26.8.2009

[RK11] S. Radack and R. Kuhn. ***Managing Security: The Security Content Automation Protocol.*** *IT Professional*, 2011, p. 9–11.

[SC08] Thomas Schmidt. ***Sicherung von Pfadvektorprotokollen mit Hilfe kryptographischer Sigantruen.*** Februar 2008. http://wcms1.rz.tu-ilmenau.de/fakia/fileadmin/template/startIA/telematik/lehre/HauptseminarTelematik/WS0708/hsws0708-bericht.pdf#page=69 [Stand: 23.5.2011]

[SM09] Jack Suess, Kevin Morooney. ***Identity Management & Trust Services.*** *EDUCAUSE Review,* vol. 44, no. 5 (September/October 2009): 24–43 http://net.educause.edu/ir/library/pdf/ERM0951.pdf [Stand: 25.5.2011]

[SSP08] Joachim Swoboda, Stephan Spitz, Michael Pramateftakis. ***Kryptographie und IT-Sicherheit.*** 1.Auflage, Vieweg+Teubner, 2008. http://library.back2hack.cc/books/Security/Kryptographie_und_IT-Sicherheit_de.pdf [Stand: 12.4.2011]

[TA09] Igli Tashi. ***Regulatory Compliance and Information Security Assurance.*** International Conference on Availability, Reliability and Security. 2009 http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2009.29 [Stand:31.5.2011]

[VAU08] Steven J. Vaughan-Nichols. ***Virtualization Sparks Security Concerns.*** Published by the IEEE Computer Society. August 2008 http://www.computer.org/portal/web/csdl/doi/10.1109/MC.2008.312 [Stand:16.5.2011]

[ViaD11] via donau – Österreichische Wasserstraßen-Gesellschaft mbH http://www.via-donau.org [Zugriff: 15.8.2011]

[VW10] S.Vucinic, H.P.Wegscheider. ***IT-Strategie der Via Donau 2010-2016.*** Version 2. Oktober 2010

[VW10-ZIT] S.Vucinic, H.P.Wegscheider. ***IT-Organisationshandbuch - Zentrales IT-Team.*** Version 2.0. Februar 2010

[Wei03] Hans-Joachim Weimann. ***Wurzeln der Nachhaltigkeit.*** LWF aktuell 37, S. 34-37. http://www.waldwissen.net/lernen/forstgeschichte/lwf_wurzel_nachhaltigkeit/ind

Anhang A – Kurzfassung

In den letzten Jahren entwickelte sich das Thema IT-Security zu einem immer essentielleren Bereich in Unternehmen weltweit. Ursprünglich als eine Sparte, die als nettes Add-On dient, angesehen, rückt IT-Security bei der Planung und Einrichtung von IT-Infrastrukturen innerhalb von Konzernen in das Zentrum. Diverse Umfragen in Medien zeigen, dass das Thema Sicherheit zu einer der Hauptprioritäten im Informations- und Kommunikationstechnologiebereich wird. Speziell Begriffe wie „Security Management“ und „Information Security“ rücken in den Mittelpunkt von IT-Experten in heutigen Unternehmen. Eine wesentliche Aufgabe besteht darin, adäquate IT-Architekturen, koordinierte Technologieführung und die Definition von Rollen und Verantwortungsbereichen über das ganze Unternehmen hinweg zu schaffen. Dies alles sollte unter Berücksichtigung von etablierten Security Richtlinien, Standards und Methoden ermöglicht werden. Stärken und Schwächen bestehender Systeme müssen analysiert werden, um notwendige Korrekturen durchzuführen und eine kontinuierliche Verbesserung sowohl der IT-Landschaft als auch des Sicherheitsbewusstseins innerhalb der Unternehmen zu gewährleisten.

Zielsetzung dieser Masterarbeit ist die Schaffung eines nachhaltigen IT-Security Managementkonzepts für kleine und mittlere Unternehmen (KMU). Dies erfolgt unter Berücksichtigung der im deutschsprachigen Raum meistverbreiteten existierenden Planungsansätze der IT-Security. Zu diesen zählen die ISO-2700x Normreihe, der IT-Grundschutzkatalog bzw. die IT-Grundschutzvorgehensweise des Bundesamt für Sicherheit in der Informationstechnik (BSI), in Österreich das österreichische Informationssicherheitshandbuch, sowie der Common Criteria for Information Technology Security Evaluation Standard (CC) zur Bewertung der Sicherheit von Informationstechnologie.

Aufbauend auf die existierenden Planungsansätze sowie die in der Arbeit identifizierten bestehenden und zukünftigen Herausforderungen für den Entwurf eines IT-Security Managementkonzepts für KMUs werden Anforderungen dafür abgeleitet. Diese werden in weiterer Folge in ein Konzept eingearbeitet, welches sicherstellt, dass mit vertretbarem Aufwand ein umfassender und nachhaltiger Beitrag zur Verbesserung der IT-Security in KMUs gewährleistet werden kann. Der nachhaltige Beitrag wird unter anderem dadurch garantiert, dass neben der Berücksichtigung existierender

Planungsansätze und Best Practices, Trends hinsichtlich der IT-Security, die in den nächsten 3-4 Jahren immer mehr an Bedeutung gewinnen werden, ebenfalls berücksichtigt sind. Es wird kleinen und mittleren Unternehmen ein einfaches Vorgehenskonzept zur Verfügung gestellt, das ihnen ermöglicht, schnell effiziente Maßnahmen zur Einrichtung eines nachhaltigen IT-Security Managements auszuwählen und durchzuführen. Die Überprüfung auf Praxistauglichkeit des entwickelten Konzepts erfolgt anschließend in Kooperation mit der ViaDonau - Österreichische Wasserstraßen-Gesellschaft mbH.

Anhang B – Abstract

In recent years the subject of IT security has developed into an essential topic in companies worldwide. Originally viewed as a nice add-on, nowadays the field of IT security is in the center of planning- and establishment activities for IT-infrastructures of any organisation. Various surveys in the media indicate that the issue of security is increasingly growing to one of the main priorities in the information and communication technology sector. Especially terms like "Security Management" and "Information Security" are moving into the focus of IT professionals in today's businesses. An essential task is to create adequate IT architectures, coordinated technology management and the definition of roles and responsibilities throughout the enterprises. This has to be done under consideration of established security policies, standards and methods. Strengths and weaknesses of existing systems must be analyzed in order to carry out necessary adjustments and to ensure a continuous improvement of the IT environment, as well as security awareness within the companies.

The objective of this thesis is to create a sustainable IT-Security Management Concept for small and medium enterprises (SMEs). It takes into account the most common existing planning approaches for IT security. These include the ISO 2700x standards, the IT-Baseline Protection Catalog (IT-Grundschutzkatalog des BSI), the IT-Baseline Protection Approach of the Federal Office for Information Security in Germany (IT-Grundschutzvorgehensweise des BSI), the Austrian Information Security Manual (Österreichisches Sicherheitshandbuch) and the Common Criteria for Information Technology Security Evaluation Standard (CC) for the security evaluation of information technology.

Based on the established planning approaches mentioned before and the identified existing and future challenges concerning the design of an IT-Security Management Concept for SMEs, the requirements are derived. Subsequently they are incorporated into a concept, which will guarantee that, with justifiable effort, a comprehensive and lasting contribution for the improvement of SMEs IT security is ensured. Moreover the lasting contribution of this work should be guaranteed considering the trends of IT security, which will get more and more influence in the next 3-4 years.

For small and medium-sized businesses a simple process concept is provided that allows them to quickly carry out effective measures for establishing a sustainable IT-Security Management. The verification of the concept on suitability for daily use is carried out in cooperation with the ViaDonau - Österreichische Wasserstraßen-Gesellschaft mbH.

Anhang C – Lebenslauf

Angaben zur Person	
Nachname(n) / Vorname(n)	**Siebenhandl Manuel, Bakk.**
Adresse(n)	Kanalstraße 4/22, 1220 Wien, Österreich
Telefon	+43 676 – 627 42 80
E-Mail	manuel.siebenhandl@gmail.com
Staatsangehörigkeit	Österreich
Geburtsdatum	22.02.1986
Schulausbildung	
1996 -2004	BG-BRG-BORG Polgarstraße 24, 1220 Wien
1992-1996	Salvatorschule – Private Volksschule mit Öffentlichkeitsrecht, Schödlbergergasse 20, 1220 Wien
Universitätsausbildung	
Oktober 2008 – Februar 2012	Masterstudium der Wirtschaftsinformatik an der Universität Wien
September 2008 – Februar 2009	Auslandsaufenthalt an der Universidad Autónoma de Madrid (Erasmus Semester)
Oktober 2004 – Oktober 2008	Bakkalaureatsstudium der Wirtschaftsinformatik an der Universität Wien und der Technischen Universität Wien mit dem Schwerpunkt „Electronic Commerce“
Berufserfahrung	
April 2009 – Dezember 2009	Zivildienst bei Caritas Socialis Gemeinnützige Privatstiftung
Juli 2006 & 2007	Ferialpraktikant bei Austria Tech – Gesellschaft des Bundes für technologiepolitische Maßnahmen GmbH
August 2005	Ferialpraktikant bei ViaDonau – Österreichische Wasserstraßen-Gesellschaft mbH
August 2004	Ferialpraktikant bei Trust Consult Unternehmensberatung GmbH