JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis

Entwicklung und Einsatz von Security Policies

Diplomarbeit zur Erlangung des akademischen Grades

Mag.rer.soc.oec

im Diplomstudium

Wirtschaftsinformatik

Angefertigt am

Institut für Informationsverarbeitung und Mikroprozessortechnik

Betreuung:

o. Univ.-Prof. Dr. Jörg R. Mühlbacher

Von:

Stefan Klement

Mitbetreuung:

Oberrat Dipl. -Ing. Rudolf Hörmanseder

Linz, November 2006

Kurzfassung

Der Grossteil der Unternehmen besitzt keine IT Security Policy, obwohl sehr viele Geschäftsprozesse mittlerweile von Informationstechnologie abhängig sind. Durch die Komplexität dieser Prozesse und verwendeten Technik wird auch Sicherheit immer komplexer und aufwendiger umzusetzen. Dabei behindern Barrieren wie Zeitaufwand, Benutzerfreundlichkeit und Akzeptanz oft die Umsetzung guter Sicherheitskonzepte. Sehr oft wird auch zu sehr in Sicherheitstechnologie und Sicherheitslösungen vertraut, ohne zu hinterfragen, ob diese richtig eingesetzt, zweckmäßig sowie ausreichend sind. Ein klassisches Beispiel wäre das täglich ausgeführte Backup, von welchem nie eine Wiederherstellung getestet wurde.

IT Security Policies stellen nun Regeln auf, was erlaubt ist und was nicht, ohne zu Beginn auf den technischen Hintergrund der verwendeten Informationstechnologie genauer einzugehen. Technologie spielt erst bei der Umsetzung eine Rolle, wenn es darum geht, die definierten Ziele zu erreichen. Dabei steht der Security Policy Prozess im Vordergrund.
Die Diplomarbeit erläutert verschiedene Typen von Security Policies, zeigt den Zusammenhang zum IT Sicherheitsprozess und gibt einen Überblick über die gängigsten Normen und Standards.

Nach diesen Basisinformationen bietet ein Satz von Folien einem Sicherheitsbeauftragten die Grundlage für einen Motivations- und Überblicksvortrag über Security Policies. Dieser Vortrag ist ausgelegt für das Management von kleinen und mittleren Unternehmen (KMUs) sowie Kleinstunternehmen.

Abstract

Most companies don’t use security policies although a lot of business processes are completely dependent on information technology. These processes and used technologies are getting more and more complex, and so is information security also getting more complex. Barriers like costs, usability and convenience often prevent the implementation of good security concepts. Also people very often rely in already used security technology and security solutions without proving the correct, appropriate and adequate usage of them. A good example is a daily made backup which is never tested and verified through a restore

process.

Security policies are defining rules of what is allowed and what is forbidden – without taking a closer look at the technical background of the used information technology. Technology will not play a rule until the implementation of the defined security goals. This diploma thesis illustrates different types of security policies and shows the context to the IT security process with a summary of the most used standards.

Danksagung

An dieser Stelle möchte ich mich bei meinen Eltern bedanken, die mein Studium unterstützt haben. Mein ausdrücklicher Dank gilt auch dem Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM) an der Johannes Kepler Universität Linz, dem Betreuer meiner Diplomarbeit, Prof. Dr. Jörg R. Mühlbacher sowie Herrn Dipl. Ing. Rudolf Hörmanseder.

Besonders danken möchte ich meinem Arbeitgeber und Kollegen der Ebit GmbH für die Möglichkeit und Unterstützung dieser Arbeit.

Inhaltsverzeichnis

1 Einleitung

„Wir haben doch eine Firewall und eine Bandsicherung, uns kann nichts passieren!“ So oder ähnlich lauten viele Aussagen zum Thema Sicherheit in der Informationstechnologie. Oft wird Sicherheit gleichbedeutend mit Investitionen in Hard- und Software gesetzt, ohne Überprüfung, ob diese Maßnahmen auch zufriedenstellende Ergebnisse liefern. Die Sicherheit von Informationen wird jedoch immer wichtiger, unter anderem auch je mehr Geschäftsvorgänge über Informationstechnologie abgewickelt werden. Gleichzeitig steigen damit auch die potentiellen Gefahren, unter anderem durch vorsätzliche Handlungen, oder einfach durch technisches Versagen.

Auch die Zeit zum Patchen von Systemen wird immer kürzer, da Schwachstellen immer schneller ausgenützt werden. Die Zeitspanne zwischen Veröffentlichung einer Schwachstelle, und der Existenz eines ersten Exploits dauerte im ersten Halbjahr 2004 nur mehr sechs Tage.

Auszüge aus dem Internet Security Threat Report[1] von Symantec [Sym04], Trends im ersten Halbjahr 2004 (gekürzt):

- *Symantec verzeichnete über 1.237 neue Schwachstellen in der ersten Jahreshälfte. Das entspricht durchschnittlich 48 Schwachstellen pro Woche, zirka 7 neuen Schwachstellen pro Tag.*
- *Symantec registrierte mehr als 4.496 neue Windows-Viren und -Würmer im Untersuchungszeitraum (vor allem Win32 war betroffen): Das ist viereinhalb Mal so viel wie im Vergleichszeitraum 2003.*
- *Adware[2] wächst sich zum handfesten Problem aus. Sechs der Top 50-Schädlinge wurden als Adware identifiziert.*

[1] Liefert alle sechs Monate eine Analyse aktueller Internetbedrohungen

[2] Software, die dem Benutzer zusätzliche Werbung in Form von Bannern oder Popups zeigt.

1.1 Aufgabenstellung und Zielsetzung

Mittels Security Policies kann ein Sicherheitsmaßstab festgelegt und die Einhaltung verifiziert werden. Ziel der Diplomarbeit ist es, die Entwicklung von Security Policies und deren Einsatz zu veranschaulichen. Dabei werden bestehende Vorgehensmodelle und Normen miteinbezogen.
Die Arbeit soll jedoch keine Sammlung von IT-Sicherheit Tipps und auch kein Sicherheits-Nachschlagewerk sein.

1.2 Aufbau der Arbeit

In einem allgemeinen Teil werden zuerst Bezeichnungen und Definitionen erklärt. Es werden die Gefahren der IT definiert, und der Einsatzzweck von Security Policies erläutert. Dabei wird auch auf die Kosten im Vergleich zum Nutzen eingegangen. Weiters werden Vorgehensmodelle vorgestellt sowie bestehende Normen und Standards wie das IT - Grundschutzhandbuch oder die ISO 17799 verglichen. Ein allgemeines Beispiel veranschaulicht die Entstehung einer Security Policy, in einem tiefergehenden Beispiel aus der Praxis werden die Detaillierungsgrade erläutert. Ein Security Policy Tutorial soll die Unterschiede für die verschiedenen Benutzergruppen aufzeigen und wie IT Sicherheitsverantwortliche Policies umsetzen können.

Der Glossar im Anhang an die Arbeit legt einerseits Begriffe fest, um Klarheit über deren Verwendung zu schaffen. Auch bietet das Glossar eine Art Übersetzungshilfe für englische Fachbegriffe, deren deutsche Übersetzung nicht eindeutig oder im allgemeinen Sprachgebrauch ist. Generell werden in der Arbeit englische Begriffe verwendet, sofern sie sich auch im Deutschen durchsetzen konnten (z.B. „E-Mail“ und nicht „elektronischer Brief“, jedoch „Risiko Analyse“ anstatt „risk analysis“).

1.3 Motivationsbeispiel: Backup Policy der Diplomarbeit

Da die Diplomarbeit über Security Policies handelt, soll auch beim Erstellen dieser eine selbst auferlegte Policy beachtet werden. Diese Policy ist naturgemäß relativ einfach und leicht verständlich. Wesentlich bei Policies ist jedoch die „Schriftform“, also das Vorliegen eines Policy-Dokumentes. Somit eignet sich diese einfache Policy sehr gut als einführendes Beispiel.
Die Diplomarbeit wurde auf einem Firmenlaptop geschrieben und war somit unter anderem folgenden potentiellen Gefahren ausgesetzt:

- Hardwaredefekt durch unsachgemäße Behandlung des Laptops, defekte Festplatte
- Verlust des Laptops durch Diebstahl
- Verlust der Daten durch schädlichen Programmcode wie Viren oder Würmer
- Verlust der Dokumente durch Fehler im Textverarbeitungsprogramms oder Betriebssystem.

Diesen Gefahren wurde das größte Bedrohungspotential zugewiesen und daraus folgende Policy definiert:

Laptop Backup Policy

Besitzer

Der Besitzer dieser Laptop Backup Policy ist Stefan Klement

Gültigkeit

Die Policy ist ab sofort gültig bis zur Abgabe der Arbeit

Verantwortlichkeit

Für Umsetzung und Durchführung der Policy ist der Verfasser selbst zuständig

Zweck

Diese Policy legt fest, wie periodische Backups von Benutzerdaten durchgeführt werden um sie gegen Datenverlust und Zerstörung zu schützen.

Wirkungsbereich

Die Policy gilt für privat genutzte Laptops und die darauf gespeicherten Benutzerdaten, außerhalb des firmeneigenen Netzwerkes. Verantwortlich für die Sicherung der Daten ist der jeweilige Benutzer selbst.

Policy Statement

- Sicherungen müssen regelmäßig auf andere Datenträger durchgeführt werden.
- Die Frequenz der Sicherung muss mit der Wichtigkeit der Daten übereinstimmen.
- Die Sicherungen müssen regelmäßig getestet werden.
- Sicherungsmedien müssen an einem dafür geeigneten Ort aufbewahrt werden.

Policy Procedure

- Während Daten verändert werden muss stündlich eine Kopie der bearbeiteten Dokumente gemacht werden. Dies soll bei Programmfehlern der Textverarbeitung Datenverlust verhindern. Dazu ist bei MS Word die Einstellung „Sicherheitskopie immer erstellen“ und „AutoWiederherstellen-Info speichern alle 60min“ im Menü „Extras/Optionen“ zu treffen.
- Nach Abschluss der Tätigkeiten an einem Tag muss eine Kopie der veränderten Daten auf einen anderen Datenträger erstellt werden. Dazu kann das Freeware Programm „Allway Sync“ (http://www.allwaysync.com) verwendet werden, welches eine Synchronisation mit einem externen Datenträger (externe Festplatte, USB Stick) durchführen kann.
- In wöchentlichen Abständen muss eine Sicherung des gesamten Datenbestands auf einen Datenträger erfolgen welcher nicht überschrieben werden kann. Dafür kommt das Sicherungssystem der Ebit GmbH zum Einsatz, welches regelmäßig Sicherungen

mit einem LTO2 Bandlaufwerk erstellt. Diese Bänder werden extern in einem dafür vorgesehenem Safe gelagert.

- Die Sicherungen müssen regelmäßig auf Korrektheit überprüft werden. Dies geschieht bei den lokalen Kopien durch Öffnen der Datei. Vom externen Datenträger wird in monatlichen Abständen versucht, alle Daten zurückzukopieren. Das nicht überschreibbare Bandbackup der Ebit GmbH erfolgt mit einer Backupsoftware, welche den gesicherten Datenbestand nach der Sicherung auf Korrektheit und Lesbarkeit überprüft.

- Bei den verschiedenen Sicherungsmaßnahmen braucht nicht auf Geheimhaltung Rücksicht genommen werden, die Datenhaltung am Firmenlaptop und Firmenbackup ist ausreichend, da die Arbeit veröffentlicht wird.

Anmerkung: Diese Policy wurde nach dem SANS Standard [Sans05] erstellt, welcher in Folge genauer erklärt wird.

2 Security Policy Grundlagen

Die Security Policy ist für ein IT Sicherheitskonzept das grundlegende Element, welches Richtungen und Ziele definiert. Sie kann mit der Sicherheitspolitik einer Regierung verglichen werden, welche Pläne und Strategien gegen mögliche und vorhandene Bedrohungen festlegt. Erst aufgrund dessen können Maßnahmen definiert werden. Solange die Strategie nicht festgelegt wurde kann nicht entschieden werden, welche Schutzmaßnahmen sinnvoll und adäquat sind, da jedes Unternehmen wie auch jedes Land andere Sicherheitsvorstellungen hat.
Mittlerweile allgemein bekannt ist, dass jedes Unternehmen eine IT Security Policy braucht. Oft werden in diesem Zusammenhang andere Bezeichnungen gewählt wie „Sicherheitsrichtlinie“, „IT - Sicherheit“ oder die deutsche Übersetzung „Sicherheitspolitik“. Behandelt werden dabei jedoch immer folgende oder ähnliche Fragen:

- Wer ist für was zuständig? (Entwurf, Umsetzung, Implementierung, Kontrolle ..)
- Warum lauten die Regeln so?
- Wie kann festgestellt werden welche Maßnahmen sinnvoll sind?
- Was ist erlaubt, was nicht, und wieso?
- Welche Zugriffe auf welche Ressourcen bekommen die Benutzer?
- Wie lauten die Netzwerk-, Antivirus-, Backup-, Sicherheitsregeln?

Durch die Security Policy wird das Sicherheitsniveau definiert, sie legt die angestrebten Sicherheitsziele und Sicherheitsstrategien fest. Wichtig dabei ist, dass zuerst das „Warum“ behandelt wird, und erst in einem weiteren Schritt das „Wie“, also welche Maßnahmen zum Einsatz kommen sollen.

2.1 Definition

Literatur und Praxis verwenden leider oft verschiedene Begriffe für IT Security Policies, umgekehrt wird auch oft unter Security Policy etwas anderes verstanden.

Folgende Definitionen sind am geläufigsten:

Security Policy

„*Documentation of computer security decisions*“ [Nist95, S. 33]

„*Published document (or sets of documents) in which the organization‘s philosophy, strategy, policies and practices with regard to confidentiality, integrity and availability of information and information systems are laid out.*” [Sec01]

Das deutsche Bundesamt für Sicherheit in der Informationstechnik [Bsi05] übersetzt „*Information Security Policy*“ mit „*IT-Sicherheitsleitlinie*“ und definiert sie folgendermaßen: „*Die IT-Sicherheitsleitlinie definiert das angestrebte IT-Sicherheitsniveau, mit dem die Aufgaben durch die Organisation erfüllt werden. Die IT-Sicherheitsleitlinie beinhaltet die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie.*“

Das mit dem deutschen Grundschutzhandbuch verwandte österreichische IT-Sicherheits-handbuch [Sihb04, S.14] bezeichnet die „*IT Security Policy*“ als „*IT-Sicherheitspolitik*“ mit folgender Definition:
„*Die IT-Sicherheitspolitik bildet die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen IT-Sicherheitskonzeptes. Sie stellt ein Grundlagendokument dar, das die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Methoden langfristig und verbindlich festlegt.*“

Auf windowsecurity.com wird in der Publikation “*Building and Implementing a Successful Information Security Policy*” folgende Definition verwendet [Dan03, S. 4]: „*The security policy is basically a plan, outlining what the company's critical assets are, and how they must (and can) be protected.*”

Das Makosi Vorgehensmodell [Mak03/2] verwendet diese Definition: „*Eine Sicherheits-richtlinie ist eine Sammlung von Regel und Vorgehensanweisungen, die festlegen, wie*

Sicherheit innerhalb eines Systems oder einer Organisation zu gewährleisten ist. Ziel dabei ist der Schutz der betroffenen Ressourcen.
Sicherheitsrichtlinien sind essenzielle Komponenten von Sicherheitsarchitekturen. Sicherheitsrichtlinien werden informationstechnisch mit Hilfe von Sicherheitsdiensten auf Basis von Regelwerken implementiert. Diese Regelwerke beschreiben die Zuordnung von sicherheitsrelevanten Objekten (engl.: prinzipals) bzw. Attributen zu erlaubten Aktionen."

Selbst zusammengefasst ist folgende Definition kurz und prägnant:

„Security Policies sind Dokumente welche Regeln enthalten, die festlegen, was erlaubt ist und was nicht, um Informationssicherheit zu definieren und zu erreichen"

2.2 Aufbau einer Security Policy nach SANS

Um eine Policy effektiv und durchführbar zu halten, sind einige wichtige Vorraussetzungen notwendig. Dies betrifft sowohl die administrativen Teile – wer ist zuständig für Inhalt, Umsetzung und Kontrolle – als auch den Inhalt der Kernaussage und der festgelegten Regeln.

Wichtigstes Element ist das Policy Statement, welches den eigentlichen Zweck beschreibt, und auch als Motivation dienen soll. Weiters legt es den Wirkungs- und Gültigkeitsbereich fest, ebenso wird die Verantwortung zur Durchführung der Policy definiert. Ein weiterer und wichtiger Teil des Statements sind die Konsequenzen bei Verstoß gegen die Policy. Als Beispiel kann hier die Dokumentensicherheit angeführt werden: Ein Unternehmen will zumeist verhindern dass firmeninterne Dokumente das Unternehmen verlassen. Dies komplett zu unterbinden ist in Zeiten des Internets, immer leistungsfähigerer und kleinerer, portabler Hardware nicht möglich. Dokumente können sowohl über Speichermedien wie USB-Sticks, CD-ROMs, auf Laptops und PDAs nach außen gelangen als auch über das Internet mittels Freemail Diensten, FTP, Instant Messaging und Filesharing Programmen. Ebenfalls sehr schwer verhindert werden kann ein Missbrauch des E-Mail Systems des Unternehmens, oder einfach ein mitgenommener Ausdruck von sensiblen Daten. Werden nun Konsequenzen festgelegt, steigt die Barriere gegen verbotene Handlungen. Natürlich muss auch genau beschrieben sein, was verboten ist, weshalb, und dies den betroffenen Personen auch mitgeteilt werden – in Form einer Security Policy.

Das seit 1989 existierende SANS Institute definierte als erstes den Begriff Security Policy und führte eine Unterteilung der Policy in [Sans05] **Statement**, **Guidelines**, **Standards** und **Procedures** ein.

2.2.1 Security Statement

Das Statement als zentrales Element einer Security Policy soll die Vorgaben des IT Managements wiedergeben und die gewünschten Sicherheitsziele beschreiben. Dabei wird sehr allgemein vorgegangen und es werden noch keine technischen Details oder Sicherheitseinstellungen konkretisiert. Vorgaben für das Security Statement können unter anderem aus einer Risiko-Analyse stammen, in welcher kritische Geschäftsprozesse und IT-Ressourcen erkannt werden. Auf die Risiko-Analyse, Bedrohungen und Risiken wird in Kapitel 3 genauer eingegangen.

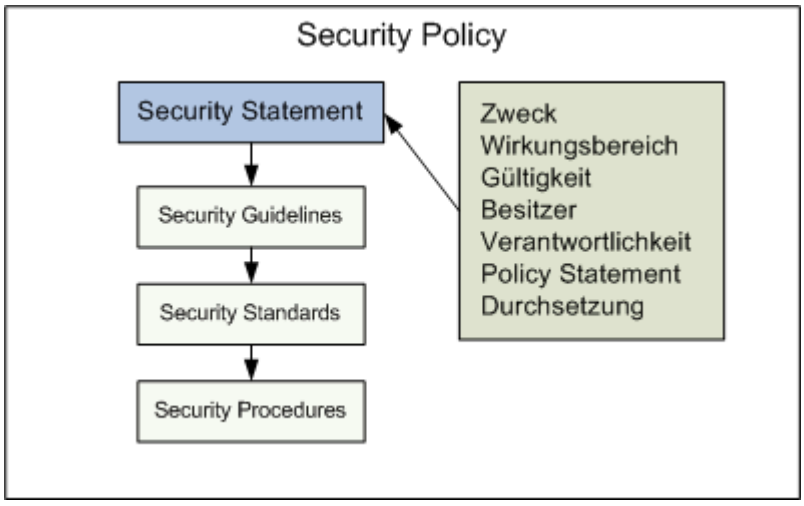


Abbildung 1: Inhalte einer Security Policy

Das Security Statement umfasst dabei folgende Punkte[3]:

Zweck (Purpose)
Der eigentliche Zweck der Policy ist die Motivation zur Steigerung der Akzeptanz. Dieser erste Punkt des Policy Statements soll dem Leser kurz und einprägsam erklären, wozu die

[3] Für ein besseres Verständnis werden deutsche Begriffe verwendet und die in der vorwiegend englischen Literatur benutzten Wörter in Klammer angegeben.

Policy verfasst wurde und was damit erreicht werden soll. Dabei soll die Aufmerksamkeit nicht durch lange Erklärungen leiden, sondern im Gegenteil die Motivation zum Weiterlesen gegeben werden.

Wirkungsbereich (Scope)
Gibt die Organisationseinheit oder Ressource an, auf die sich die Policy bezieht. Dabei kann es sich um alle Personen eines Unternehmens handeln, eine Abteilung oder einen geschlossenen Benutzerkreis wie Administratoren oder Außendienstmitarbeiter. Auf Hardwareseite können dies alle PCs, Server, Firewalls oder mobile Geräte sein. Beispiele für Policies, welche meist für alle Personen gelten, sind die Acceptable Use Policy oder die Anti-Virus Policy. Eine Remote Access Policy oder Server Security Policy sind spezialisierter und gelten nur für einen kleineren Wirkungsbereich.

Gültigkeit (Validity)
Meist hat die Policy eine begrenzte Gültigkeit, nach deren Ablauf ein Review prüfen soll, ob die Policy angepasst werden muss. Dies kann notwendig werden, wenn sich Vorgaben oder Rahmenbedingungen ändern. Beispiele dafür sind neue Hardware, veränderter Einsatzzweck einer IT-Komponente oder ein geändertes Sicherheitsbedürfnis des Unternehmens.

Besitzer (Ownership)
Legt fest, wer für Änderungen im Dokument zuständig ist. Es darf nur eine Person Besitzer des Dokumentes sein und dieses ändern.

Verantwortlichkeit (Responsibilities)
Gibt an, wer für die Umsetzung und Durchführung der Policy verantwortlich ist. Anstatt jeder Policy einzeln eine konkrete Person zuzuweisen, ist es meist sinnvoller, Rollen zu definieren und diesen Rollen die Verantwortlichkeit zu geben. Eine Rolle könnte zum Beispiel sein „Anti-Virus Officer“ oder „Netzwerk und Firewall Officer“. Jede dieser Rollen ist von einer verantwortlichen Person wahrzunehmen (Vergleichbar mit dem Rollenkonzept bei Datenbanken).

Policy Statement
Die eigentliche Aussage. Das Statement konkretisiert „Was“ geschützt werden soll, und nicht das technische „Wie“. Dies wird durch die Procedures beschrieben.

Durchsetzung (Enforcement)
Konsequenzen bei Verstoß gegen die Policy, welche von Ermahnungen bis hin zu disziplinären Maßnahmen gehen kann. Bei beabsichtigten Handlungen wie Weitergabe von vertraulichen Daten oder Diebstahl sollte auf zivilrechtliche Konsequenzen hingewiesen werden. Das Veröffentlichen solcher Konsequenzen verhindert zu einem gewissen Prozentsatz Verstöße, da eher mit einer eventuellen Bestrafung gerechnet wird. Zu viele explizite Verbote sollten aber vermieden werden, um nicht den Eindruck zu erwecken, dass fast nichts erlaubt ist und dadurch Übertretungen nicht mehr ernst genommen werden.

Meist wird nicht genau diese Unterteilung einer Policy benutzt, welche bei Beispielpolicies von [Sans05] verwendet wird, sondern oft werden einige Punkte zusammengefasst oder weggelassen. In der Literatur ist auch nicht genau festgelegt, welche Elemente vorkommen sollten, dafür gibt es zu viele verschiedene Auffassungen und Ansätze. Das Statement an sich, die Verantwortlichkeiten und der Wirkungsbereich werden jedoch fast immer angegeben, denn ohne diese Punkte wäre der Inhalt der Policy nicht richtig anzuwenden.

2.2.2 Security Guidelines

Guidelines sind Empfehlungen und Vorschläge, deren Einhaltung jedoch dringend empfohlen wird. Oft finden sich solche Auflistungen von Empfehlungen unter den Begriffen „How-to“ oder „Best Practice“. Werden Guidelines allgemein anerkannt und etablieren sich als gängige Maßnahmen, werden sie oft als Standards definiert. Die Policy verweist meist auf Guidelines wie auch auf Standards.
Guidelines werden unter anderem erstellt für:

- **Passwort Guideline:** Definiert, wie Passwörter ausgewählt werden sollen und zeigt Beispiele für gute (und schlechte) Passwörter. Die Passwort Guideline kann auch Vorgaben umfassen, wie viele Zeichen ein Passwort mindestens lang sein muss und aus welchen verschiedenen Zeichengruppen (Grossbuchstaben, Ziffern, Sonderzeichen) Zeichen vorkommen sollen.

- **Backup Guideline:** Fasst Vorgaben für die Datensicherung zusammen, um ein zuverlässiges Backup zu gewährleisten. Dies kann die Backupmethoden, Backuphäufigkeit und Backupmedien umfassen.

- **Server Setup Guideline:** Dies sind Empfehlungen zum Aufsetzen von Server-Betriebssystemen, z.B. eine „Windows Server 2003 Setup Guideline“. Die Guideline beschreibt Parameter wie Partitionsgrösse, Raid-Levels und Hardware Ausstattung.

- **Logging Guideline:** Log Informationen werden an verschiedenen Stellen des Betriebssystems gespeichert wie z.B. im Event Log oder Logfiles. Wo genau diese Logfiles sind, was geloggt werden soll und wann ein Log überschrieben werden kann sind Inhalte der Logging Guideline.

Beispiel für eine Passwort Guideline:

- Passwörter enthalten Gross- und Kleinbuchstaben (a-z, A-Z).

- Es muss mindestens eine Ziffer oder ein Sonderzeichen vorkommen (0-9, !§$@)

- Die minimale Passwortlänge ist 9 Zeichen.

- Das Passwort darf in keinem Wörterbuch stehen und keinen Bezug zu persönlichen Informationen, wie Geburtsdaten oder Namen von Familienmitgliedern haben.

- Passwörter dürfen nicht aufgeschrieben werden oder unverschlüsselt gespeichert werden.

- Man sollte Passwörter so wählen dass sie einfach zu merken sind. Praktisch hierfür ist zum Beispiel der Anfangsbuchstabe eines jeden Wortes eines Satzes: „Heute muss ich mein Passwort schon wieder ändern!“ wird dann zu „:-(HmimPswä!“

2.2.3 Security Standards

Security Standards sind Sammlungen von spezifischen Anforderungen die eingehalten werden müssen. Ein Standard sollte ein eigenes Dokument sein auf welches aus der Policy verwiesen werden kann.

Das SANS Institute beschreibt Standards folgendermaßen [Sans05]:

“*A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to harden a Windows NT workstation for placement on an external (DMZ) network. People must*

follow this standard exactly if they wish to install a Windows NT workstation on an external network segment."

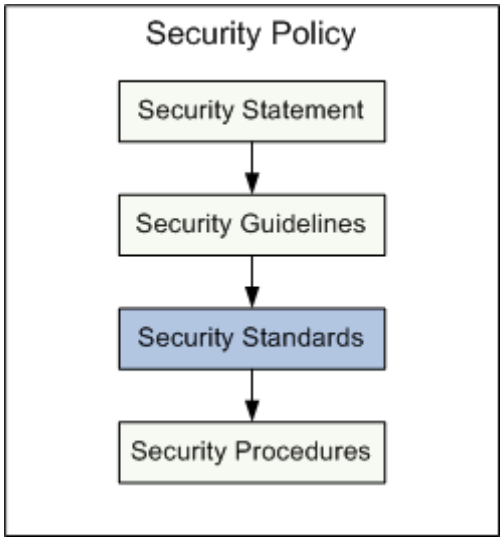


Abbildung 2: Security Policy - Standards

Auszug aus einem Passwort Policy Standard [Sans05], gekürzt:

- *Passwörter dürfen nicht weitergegeben werden, auch nicht an Helpdesk Mitarbeiter oder Kollegen.*
- *Passwörter dürfen niemals über das Telefon oder Klartext in einem Mail weitergegeben werden.*
- *Wenn Passwörter mündlich weitergegeben werden muss darauf geachtet werden dass keine anderen Personen zuhören.*
- *Die Funktion „Passwort speichern" von verschiedenen Applikationen und Browsern darf nicht verwendet werden.*
- *Passwörter dürfen nicht unverschlüsselt gespeichert werden, weder auf PCs, Servern oder PDAs.*

Man soll bereits bestehende Standards und Normen verwenden und diese bei Bedarf im Rahmen der Security Procedures anpassen und konkretisieren. Zu den wichtigsten Standards im Bereich IT Security zählen das Österreichische IT-Grundschutzhandbuch, das deutsche IT-Grundschutzhandbuch, die Normen ISO 17799 und ISO 13335 sowie ITSEC und Common

Criteria. Wie diese Normen und Standards für IT Security Policies verwendet werden können, ist in Kapitel 4:“Normen und Standards“ beschrieben.

2.2.4 Security Procedures

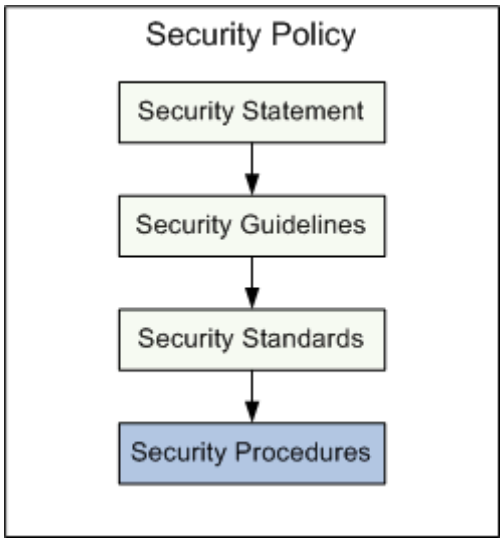


Abbildung 3: Security Policy - Procedures

Security Procedures sind genaue Vorgehensweisen für verschiedene Aufgaben wie Einstellungen eines Virenscanners oder der Ablauf bei Verdacht auf einen aktiven Virus. Dabei werden Schritt für Schritt Anweisungen definiert, was in einem gewissen Fall zu tun ist. Die Procedures sind im Vergleich zu Statements, Guidelines und Standards technologieabhängig. Sie beschreiben, wie etwas umzusetzen ist und sind somit der letzte Schritt bei der Erstellung einer Security Policy.

Beispiele dazu sind Backup Procedure, Anti Virus Procedure, Router Security Procedure oder Incident Handling Procedure.

Eine „Backup Procedure“ für Backup-Administratoren könnte folgende Punkte enthalten:

- Das Backup vom Vortag muss täglich bis 10:00 durch Einsicht in das Backup-Log kontrolliert werden. Ein fehlerhaftes Backup (CRC Fehler, Abbruch ...) muss sofort dem IT-Sicherheitsverantwortlichen durch mündliche Miteilung (unter Tel. DW 2441) gemeldet werden.

- Bis 16:00 sind alle Backupbänder für das Backup am aktuellen Tag laut Backup-Liste 1 einzulegen. Das Wechseln des Bandes ist per Unterschrift in dieser Liste zu bestätigen.

- Die Bänder vom Vortag sind ordnungsgemäß zu verwahren. Tages- und Wochenbackupbänder werden in dem dafür vorgesehenen Safe im Raum T664 aufbewahrt. Monatsbackups werden am nächsten Werktag nach dem Backup in das Bankschließfach Nr. 880 gebracht.

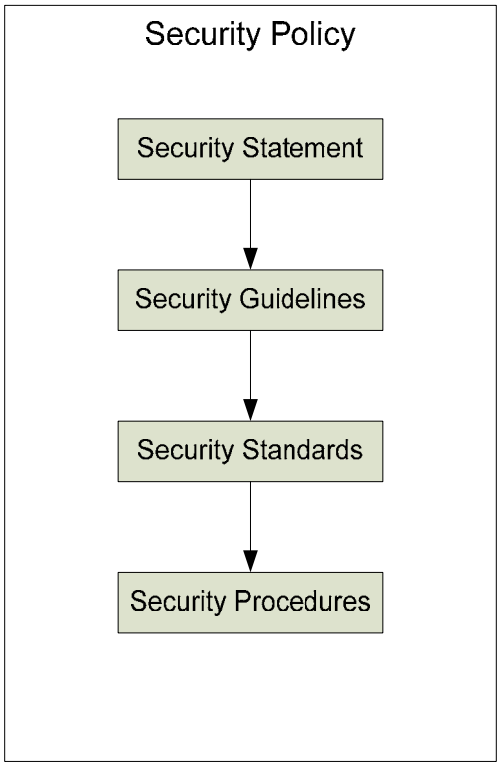
- Bei der Auslagerung der Monatsbackupbänder ist die Entnahme aus dem Safe in der dafür vorgesehenen Liste einzutragen. Der Bank-Safeschlüssel ist bei Hr. Müller zu übernehmen, die Übernahme zu bestätigen, und nach Auslagerung der Bänder wieder zu retournieren.

- Der Verwahrungsort der Backupbänder unterliegt der Geheimhaltung.

Das CERT Coordination Center definiert Security Procedures folgendermaßen [Cert97]: "*Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.*"

2.2.5 Zusammenhang der einzelnen Teile

Der Zusammenhang der einzelnen Teile einer Security Policy ist in folgender Grafik ersichtlich:



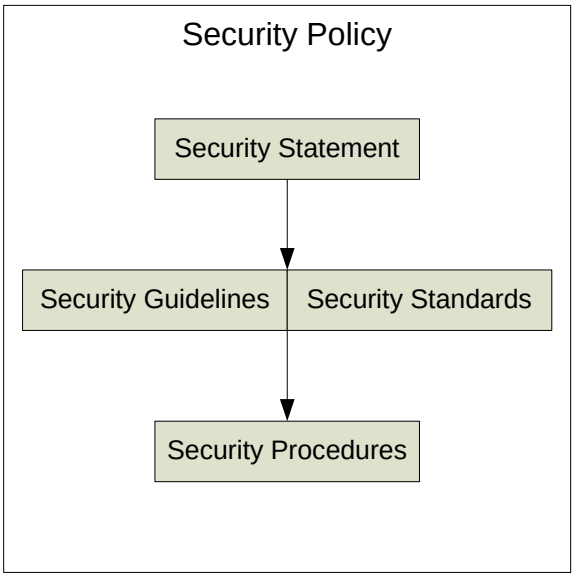


Abbildung 4: Elemente einer Security Policy **Abbildung 5: Elemente einer Security Policy, vereinfacht**

Eine Policy beginnt somit immer mit dem eigentlichen Statement. In diesem kann auf Guidelines und Standards verwiesen werden. Zum Schluss legen die Procedures die konkreten technischen Abläufe und Vorgangsweisen fest.

Meist existieren Teile einer Policy bereits in einem Unternehmen, jedoch oft nur in mündlicher Form oder einfach aus Gewohnheit heraus. Eine echte Policy definiert sich aber dadurch, dass sie in schriftlicher Form vorliegt. Dies bringt eine bessere Übersicht über die einzuhaltenden Regeln als auch einfachere Umsetzung und Kontrolle.

Eine Security Policy, welche alle Abstraktionsstufen ausführlich behandelt, ist eher die Ausnahme. Die meisten Policies befassen sich nur mit den wichtigsten Teilen, oft in einem Dokument vermischt.

Der Weg, von einer Guideline zu einem Standard zu gelangen wird nicht sehr oft ausgeführt. Es wird meist auf bereits bestehende Guidelines oder Standards verwiesen. Dies können sowohl interne Dokumente als auch öffentliche Normen sein. Berücksichtigt man dies, ergibt sich eine leicht vereinfachte Übersicht welche in Abbildung 5 ersichtlich ist.

2.3 Aufbau einer Security Policy nach österreichischem IT-Sicherheitshandbuch

Das Österreichische IT-Sicherheitshandbuch verwendet folgende Unterteilung von Security Policies [Sihb04, S. 56-58, gekürzt]:

„IT-Systemsicherheitspolitiken

Aufgaben und Ziele

Eine IT-Systemsicherheitspolitik stellt ein Basisdokument dar. In diesem

- werden die grundlegenden Vorgaben und Leitlinien zur Sicherheit in einem IT-System definiert.
- sind Details über die ausgewählten Sicherheitsmaßnahmen beschrieben und
- werden die Gründe für die Auswahl der Sicherheitsmaßnahmen dargelegt.

IT-Systemsicherheitspolitiken sollten für alle komplexen oder stark verbreiteten IT-Systeme erarbeitet werden. Typische Beispiele sind etwa eine PC-Sicherheitspolitik, eine Netzsicherheitspolitik oder eine Internet-Sicherheitspolitik.

Inhalte

Eine IT-Systemsicherheitspolitik soll Aussagen zu folgenden Bereichen treffen:
- Definition und Abgrenzung des Systems, Beschreibung der wichtigsten Komponenten
- Definition der wichtigsten Ziele und Funktionalitäten des Systems
- Festlegen der IT-Sicherheitsziele des Systems
- Gründe für die Auswahl der Maßnahmen
- Verantwortlichkeiten

Fortschreibung der IT-Systemsicherheitspolitiken

Auch eine IT-Systemsicherheitspolitik stellt kein einmal erstelltes, unveränderbares Dokument dar, sondern ist regelmäßig auf Aktualität zu überprüfen und bei Bedarf entsprechend anzupassen.

Verantwortlichkeiten

Die Verantwortlichkeiten für die Erstellung und Fortschreibung der IT-Systemsicherheitspolitiken sind im Einzelnen in der IT-Sicherheitspolitik festzulegen.“

Die Inhalte der IT-Systemsicherheitspolitiken des Österreichischen Sicherheitshandbuchs decken sich mit Teilen der Security Policies bei SANS, besonders bei der Form des Dokumentes, der Gültigkeit und den Verantwortlichkeiten. Es ist nicht notwendig dass eine Policy vollständig alle Punkte abdeckt. Wichtiger ist, dass überhaupt eine Policy zu einem sicherheitsrelevanten Thema existiert und dieses Thema behandelt wird.

Zusammenfassend kann man sagen, dass der Aufbau der Security Policies bei SANS ein aufgabenbezogenes Framework ist und beim österreichischen IT-Sicherheitshandbuch ein systembezogener Ansatz verwendet wird.

Bei Systembezogenen Frameworks wie dem österreichischen IT-Sicherheitshandbuch oder dem deutschen Grundschutzhandbuch wird durch Standard-Sicherheitsmaßnahmen (technisch, infrastrukturell, organisatorisch) ein bestimmtes Sicherheitsniveau für IT-Systeme erreicht. Dabei sind Kataloge mit Maßnahmen zur Erreichung des Sicherheitsniveaus vorhanden.

Aufgabenbezogene Frameworks beziehen sich nicht direkt auf das Gesamtsystem sondern auf einzelne Produkte oder Komponenten und stellen keine fixen Kataloge bereit. Sie geben eher nur den groben Rahmen für die Erstellung und Inhalte der Security Policies vor.

2.4 Typen von Security Policies

Generell könnte es ein Dokument geben mit allen sicherheitstechnisch relevanten Regeln und Richtlinien zu allen Bereichen. Dies wäre jedoch schnell unübersichtlich. Weiters sind für Policies oft unterschiedliche Personen für den Inhalt und die Aktualisierung verantwortlich, ebenfalls gelten Policies für verschiedene Zielgruppen. Deshalb wird fast immer in kleinere Policies unterteilt. Dabei empfiehlt sich der Top-Down Ansatz: Zuerst wird eine allgemeine Unternehmensweite Policy (Corporate IT Security Policy) entworfen, welche von der Firmenleitung in Kraft gesetzt wird. Darunter werden Policies für einzelne Bereiche wie Laptopsicherheit, Datensicherung oder E-Mail Sicherheit geschrieben.

2.4.1 Corporate IT Security Policy

Die Corporate Security Policy stellt das Basisdokument bei der Entwicklung von Security Policies dar. Sie ist die erste Policy, die verfasst werden muss, und umfasst folgende Inhalte [Sihb04, S 14]:

- *IT-Sicherheitsziele und –strategien*
- *Organisation und Verantwortlichkeiten für IT-Sicherheit*
- *Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz*
- *Klassifizierung von Daten*
- *Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung*
- *Aktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit*

Wie jedes andere Policy Statement kann auch die Corporate Security Policy nach der unter 2.2.1 beschriebenen Struktur, mit folgenden Besonderheiten, eingeteilt werden:

Zweck
IT-Sicherheit im Unternehmen, Sicherheitsmanagement, Sensibilisierung

Wirkungsbereich
Alle Mitarbeiter, gesamtes Unternehmen

Gültigkeit

bis auf Widerruf oder einem bestimmten Datum

Besitzer

Geschäftsführung, Vorstand

Verantwortlichkeit

IT-Sicherheitsbeauftragter, IT-Sicherheitsteam

Statement

Unternehmensleitsätze, grundlegende Regeln zur IT-Sicherheit, Unternehmensphilosophie und Leitbild

Durchsetzung

generelle Maßnahmen bei leichter und grober Fahrlässigkeit oder absichtlich schädigenden Handlungen

2.4.2 Systembezogene IT Security Policies

Abhängig von der Unternehmensgröße und –struktur werden im Anschluss an die Corporate Security Policy weitere Policies verfasst. Diese Policies umfassen jeweils die Sicherheit eines IT-Systems. Tabelle 1 listet einige häufig implementierte Policies auf. Diese Policies müssen auf der Corporate Security Policy aufbauen.

Policy	Inhalt
Corporate Security Policy	Unternehmensweit gültige Sicherheitsleitsätze
Acceptable Use Policy	Korrekte Benutzung von IT Equipment und Services
E-Mail Policy	Sichere Nutzung von E-Mail
Anti-Virus Policy	Vorgaben für alle Computer um Computerviren zu erkennen und vermeiden
Passwort Policy	Sichere Passwortwahl, Aufbewahrung und regelmäßige Änderung

VPN Security Policy	Vorraussetzungen für VPN Verbindungen
Remote Access Policy	Zugriffsarten auf das Intranet von extern
Backup Policy	Beschreibt Vorgaben für die Datensicherung
Wireless Network Policy	Vorgaben für Funknetzwerke und deren Benutzung
Laptop Security Policy	Laptop Sicherheit, Umgang mit Laptops
Server Security Policy	Sicherheitsanforderungen für Server im Unternehmen
Router Security Policy	Minimale Sicherheitsanforderungen für Router und Switches
Acceptable Encryption Policy	Anforderungen an die verwendeten Verschlüsselungs-algorithmen
Public Key Infrastructure Policy	Management von Schlüsseln bei asymmetrischen Verschlüsselungsverfahren

Tabelle 1: Auflistung von Policies

Die Anzahl und Detailgenauigkeit der systembezogenen Security Policies ist stark von der Unternehmensgröße abhängig. Für kleine oder mittelständische Unternehmen sind oft einige wenige Policies ausreichend, welche sich mit dem Kern der verwendeten IT Systeme befassen. Bei nicht IT lastigen Unternehmen decken die Corporate Security Policy, Acceptable Use Policy, E-Mail Policy und Passwort Policy meist schon den Großteil der IT-Systeme ab. Große Konzerne oder Behörden besitzen eine weitaus komplexere IT Landschaft, was zu einer größeren Anzahl Policies führt.

„Abbildung 6: Security Policy Typen“ zeigt den Zusammenhang zwischen der zuerst zu erarbeitenden Corporate IT Security Policy und den darauf weiteren möglichen Policies.

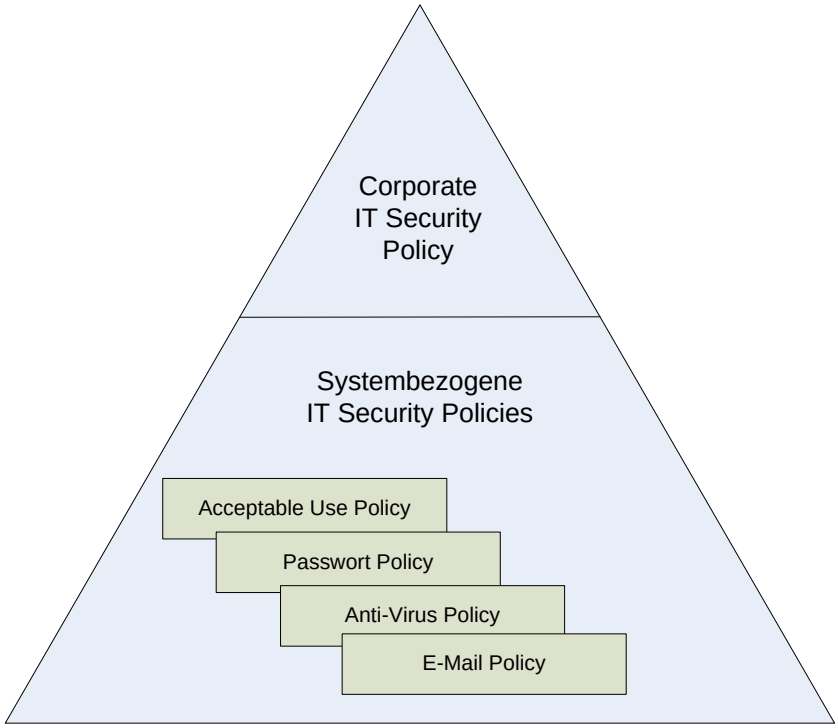


Abbildung 6: Security Policy Typen

3 IT Sicherheitsprozess

3.1 Sicherheitsziele und Sicherheitskriterien

Sicherheitsziele und Kriterien werden oftmals vermischt oder nicht klar festgelegt. Sie sind jedoch der Ausgangspunkt eines ordentlichen IT Sicherheitsprozesses und sollten genau bestimmt werden.
Definiert werden diese beiden Begriffe folgendermaßen:

„Der Begriff Ziel bezeichnet einen in der Zukunft liegenden, gegenüber dem Gegenwärtigen im Allgemeinen veränderten, erstrebenswerten und angestrebten Zustand. Ein Ziel ist ein definierter und angestrebter Endpunkt eines Prozesses, meist einer menschlichen Handlung. Mit dem Ziel ist der Erfolg eines Projekts bzw. einer mehr oder weniger anstrengenden Arbeit markiert.“ [Wiki01]

„Ein Kriterium ist ein Merkmal, das bei einer Auswahl zwischen Personen oder Objekten (Gegenständen, Eigenschaften, Themen, usw.) relevant für die Entscheidung ist.“ [Wiki02]

Ein weiterer Unterschied ist dass Ziele zumeist selbst anhand des vorhandenen Sicherheitsbedarfs definiert werden und Kriterien in Katalogen wie ITSEC[4] oder Common Criteria[5] quasi standardisiert sind. Kriterien können als Grundlage für Ziele dienen, indem die Ausprägung des Kriteriums über einen gewissen Zeitraum definiert wird und somit zum Ziel wird. So zählt die System-Verfügbarkeit zu den Sicherheitskriterien und wird durch Festlegen von maximal tolerierbaren Ausfallzeiten oder maximalen Wiederanlaufzeiten zum Ziel.

---

[4] Auf europäischer Ebene wurden die "Information Technology Security Evaluation Criteria – ITSEC" am 3. März 1998, im Rahmen des europäischen Abkommens zur gegenseitigen Anerkennung, der Zertifikate der ITSEC-Evaluation, in Kraft gesetzt. http://www.bsi.de/zertifiz/itkrit/itsec.htm

[5] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik/ Common Criteria for Information Technology Security Evaluation (CC), Version 2.0" sind im Mai 1998 unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA abschließend fertiggestellt worden. http://www.bsi.de/cc/index.htm

Auf die Unterschiede einzelner Kriterienkataloge wird im nächsten Kapitel genauer eingegangen.

Sicherheitsziele werden nun nach Festlegung des Sicherheitsniveaus für ein Unternehmen bestimmt. Sie nehmen Bezug auf Informations- und Kommunikationssysteme und deren Bedeutung für das Unternehmen. Dazu muss zuerst klargemacht werden, welche Aufgaben des Unternehmens wie stark von einem ordnungsgemäßen Funktionieren der IT Infrastruktur abhängig sind. Im Einzelnen wird also festgelegt, wie wichtig die einzelnen IT Systeme sind und welches Sicherheitsniveau sinnvoll ist.

Sicherheitsziele kann man grob in drei Kategorien unterteilen: Prävention (prevention), Erkennung (detection) und Wiederherstellung (recovery).

Prävention

Grundsätzlich sollten die meisten Sicherheitsprobleme von vornherein verhindert werden. Dies ist durch Vulnerability Management bereits sehr gut möglich, indem Patches sehr schnell installiert werden und die eingesetzte Software auf nicht geschlossene Lücken getestet wird. Eine Sicherheitslücke kann jedoch nicht geschlossen werden, bevor sie entdeckt wurde. Dies führt zu einer Zeitspanne zwischen Identifizierung und Veröffentlichung des Patches, in welcher die betroffenen Systeme verwundbar sind. Damit ist es also unmöglich, alle Sicherheitsprobleme von vornherein zu verhindern. Bedrohungen müssen aber so gut als möglich vermieden werden. Zur Prävention zählen unter anderem folgende Sicherheitsziele:

- Isolierung einzelner Netzwerkbereiche mit hohem Schutzbedarf. Wenn notwendig vollständige physikalische Trennung mit meist nur eingeschränkter Kommunikation über Firewalls.

- Sicherstellung der Datensicherung aller relevanten Systeme, Korrektheit der Datensicherung

- Verschlüsselung aller zu übermittelnden vertraulichen Informationen

- Zugriffsrechte für unterschiedliche Benutzergruppen definieren, um unberechtigte Zugriffe zu verhindern (z.B. durch Access Control Listen im Dateisystem, rollenbasierte Einschränkungen des Datenbank-Zugriffes

- Verwenden von State-of-the-Art Software gegen Schadprogramme wie Viren, Spyware oder Trojaner.

Erkennung

Da nicht alle Sicherheitsprobleme verhindert werden können ist die Erkennung von Angriffen ebenfalls sehr wichtig. Sollte es trotz aller Sicherheitsvorkehrungen einem Angreifer von extern oder einem Mitarbeiter im Unternehmen gelingen unerlaubt an Informationen zu kommen, so sollte dies zumindest entdeckt werden. Dadurch können die gefundenen Lücken beseitigt und Maßnahmen gegen den oder die Angreifer getätigt werden. Man muss sich nur darüber im Klaren sein, dass es keine perfekten Sicherheitssysteme gibt und Menschen immer versuchen werden, diese zu umgehen. Die Erkennung von Angriffen erfolgt unter anderem durch Auswerten von Logfiles welche von Firewalls, Routern, Servern und anderen Netzwerkkomponenten erzeugt werden. Nach Möglichkeit sollte dies in Echtzeit erfolgen um rasch reagieren zu können.
Zum Einsatz kommen hierbei Intrusion Detection Systeme, welche Angriffe auf Computersysteme erkennen sollen oder Loganalysatoren zur Auswertung von System-Logs auf ungewöhnliche Ereignisse wie fehlerhafte Login Versuche.

- Monitoring des Netzwerkverkehrs zur Angriffsfrüherkennung
- Automatisiertes Auswerten von fehlgeschlagenen Login Versuchen
- Erkennung von unerlaubter Datenübertragung
- Erkennen von unerlaubter Hardware (PCs, USB-Sticks, Modems, Wireless LANs ..) im Unternehmensnetz

Wiederherstellung

Als Wiederherstellung werden Maßnahmen bezeichnet, welche nach einem Hardware- oder Softwarefehler den ursprünglichen Zustand so gut wie möglich rekonstruieren sollen. Dabei spricht man von der Systemausfallszeit, welche angibt, wie lange ein IT System nicht verfügbar ist (komplette Zeitspanne des Ausfalles) und der Wiederanlaufzeit, bis das System erneut verfügbar ist (Zeitspanne welche benötigt wird um ein System wieder aktiv zu bekommen). Die Qualität der Wiederherstellung definiert sich durch die Konsistenz des

wiederhergestellten Datenbestandes, also ob nach der Wiederherstellung alle Daten korrekt sind.

Sicherheitsziele in diesem Bereich können sein:

- Bereitstellen von Ersatzhardware bei einem Defekt in einem definierten Zeitraum
- Verkürzen von Systemausfallzeiten bei sensiblen Systemen
- Überprüfen der Wiederherstellbarkeit von Daten vom Backup
- Korrektes Aufbewahren von Sicherungsmedien gegen Feuer und unberechtigtem Zugriff oder Diebstahl

Die grundlegenden **IT - Sicherheitskriterien** bestehen aus Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Sie werden auch als „Grundbedrohungen“ bezeichnet, da Bedrohungen der IT-Infrastruktur sich in diese drei Punkte einteilen lassen.

Vertraulichkeit hat mit dem Schutz von vertraulichen Daten zu tun und soll verhindern dass unautorisierte Benutzer Zugriff auf Informationen erhalten. Ein unbefugter Informationsgewinn führt somit zum Verlust der Vertraulichkeit. Bis vor einigen Jahren war die Vertraulichkeit das wichtigste Kriterium, gefolgt von Integrität und Verfügbarkeit.

Integrität bedeutet dass Daten nicht unautorisiert verändert werden können und der zuletzt gültige Zustand bestehen bleibt. Im Unterschied zu Vertraulichkeit hat Integrität mit der Sicherheit beim Schreiben von Daten zu tun.

Verfügbarkeit ist mittlerweile zum wichtigsten Kriterium geworden. Die Verfügbarkeit soll sicherstellen, dass Systeme zum richtigen Zeitpunkt an der richtigen Stelle verfügbar sind. Verfügbarkeit wird unter anderem gefährdet durch Hardwareausfälle, Denial-of-Service Absetz-Attacken oder durch Computerviren.
Mit verschiedenen Techniken können die Sicherheitskriterien besser erfüllt und somit die definierten Sicherheitsziele erreicht werden.

Einige Sicherheitstechniken sind:

- Identifizierung, Authentifikation und Zugriffskontrolle um Vertraulichkeit zu garantieren.
- Kryptografie für Vertraulichkeit und Integrität.
- Hardware zum Absichern des Netzwerkverkehrs bezüglich Vertraulichkeit, Integrität und Verfügbarkeit: Firewalls, Router, Switches
- Verhinderung von Social Engineering, z.B. durch Benutzerschulungen, verbessert Vertraulichkeit.

3.2 Bedrohungen und Gefahren

IT Systeme sind anfällig für eine Reihe von Bedrohungen und Gefahren mit unterschiedlichen Auswirkungen und Eintrittswahrscheinlichkeiten. Diese Bedrohungen können sowohl von extern als auch intern kommen, absichtlich oder zufällig entstehen, durch Unwissenheit oder mit Vorsatz getätigt werden.
Es ist wichtig, sich im Vorfeld über die verschiedenen IT Bedrohungen und Gefahren im Klaren zu werden, um im IT Sicherheitsprozess Risiken bestimmen und Gegenmaßnahmen gezielt einleiten zu können.

3.2.1 Menschliches Versagen

Der menschliche Faktor ist der am schwersten zu kontrollierende im IT Sicherheitsbereich. Selbst bei einem extrem sicheren System, welches mittels Kryptographie, strengen Sicherheitsprotokollen und ausfallsicherer Hardware geschützt ist und wenn nur fehlerfreie Software[6] eingesetzt wird, muss das System von Menschen bedient werden. Durch menschliches Fehlverhalten werden Eingabefehler gemacht, Sicherheitssysteme umgangen

[6] Ausfallsichere Hardware und fehlerfreie Software würde bedeuten, dass bei der Entwicklung dieser Systeme niemand einen Fehler gemacht hat. Diese Annahme ist bei der Komplexität heutiger IT Systeme idealistisch. Weiters könnte man diesen Ansatz so fortführen dass jegliche Fehler auf Menschen zurückzuführen sind (Hardwareausfälle, Datenverlust, ..). Diese Sicht ist aber nicht zielführend und wird nicht weiter betrachtet.

oder wird in Ausnahmesituationen falsch reagiert.
Die Gründe für menschliches Versagen können verschieden sein:

- Personeller Mangel verursacht eine Überforderung der Mitarbeiter und führt vermehrt zu Fehlern.

- Organisatorische Mängel, wie z.B. das Fehlen eines dezidierten Sicherheitsbeauftragten, zu wenig geschultes Personal oder kein durchgängiges Sicherheitskonzept (aus Kostengründen).

Sind solche Voraussetzungen gegeben, so entstehen oft falsche Konfigurationen von IT Systemen wie Betriebssystemen, Anwendungsprogrammen oder Netzwerkkomponenten. Betrifft dies Systeme, welche eigentlich der Sicherheit dienen, wie Firewalls oder Antivirus Software, kann der Fehler fatal sein, da er das zum Schutz eingeführte System anfällig macht oder sogar deaktiviert.
Das größte Risiko geht dabei von den Benutzern selbst aus, welche durch ungenügendes Wissen oder fehlenden Schulungen Sicherheitssysteme umgehen:

- Verwenden von einfachen Passwörter wie dem Vornamen

- schriftliches Aufbewahren der Passwörter am Arbeitsplatz (post-it)

- Weitergeben von Passwörtern am Telefon an unbekannte Personen

- Öffnen und Ausführen von unbekannten e-mail Attachments

- Deaktivieren von Antivirus Software

- unbeabsichtigtes Löschen von Daten

- Sorgloser Umgang mit Informationen

Nur Teile dieser Fehler können durch technische Maßnahmen verhindert werden. Zur Verbesserung der Passwort-Handhabung können z.B. Tokens wie Chipkarten eingesetzt werden, welche erst in Kombination mit dem Passwort den Zugriff auf die Ressource erlauben.

3.2.2 Technisches Versagen

Von technischem Versagen wird gesprochen, wenn ein Gerät in einem Zustand ist, in welchem es seine Aufgabe nicht mehr vollständig ausführen kann. Die Gründe hierfür sind vielfältig: Abnutzung, Systemfehler, unzureichende Wartung, Überspannung im Stromnetz, physische Zerstörung.

Technisches Versagen kann immer vorkommen, es gibt keine 100% zuverlässige Technik. Die Wahrscheinlichkeit eines Versagens wird mit der Ausfallwahrscheinlichkeit angegeben. Beispiele für technisches Versagen sind:

- Unterbrechung oder Schwankung der Stromversorgung vom Energieversorger kann zum Ausfall von IT Systemen führen, wenn diese nicht richtig abgesichert sind.

- Defekte Datenträger wie Festplatten oder Bänder: Dies kann durch mechanische Erschütterungen, Alterung bzw. Abnutzung, Magnetfelder, Staub oder Überhitzung geschehen.

- Ausfall einer Datenbank führt zum Ausfall sämtlicher Anwendungen welche diese Datenbank benutzen und kann hohen wirtschaftlichen Schaden verursachen.

- Ausfall von Sicherungseinrichtungen wie Brandschutztüren, Türschlössern oder Feuermeldern.

- Bei Ausfall von Netzwerkkomponenten wie Routern, Switches oder Firewall kommt es zum Verlust der Verfügbarkeit des Netzes.

Gegen technisches Versagen kann man sich in den meisten Fällen mit entsprechenden Maßnahmen schützen: redundante Hardware, Supportvereinbarungen, Hardware auf Reserve, regelmäßige Funktionsüberprüfungen, Austausch nach einer gewissen Laufzeit...

Da diese Maßnahmen alle kostenintensiv sind, wird oft zugunsten geringerer Ausgaben auf Ausfallsicherheit verzichtet und das Risiko eines Ausfalles in Kauf genommen. Macht man sich die Kosten eines längeren Ausfalles oder Datenverlustes bewusst, stehen diese jedoch meist in keinem Verhältnis mit der Anschaffung zusätzlicher Hardware. Auf das Thema Risikomanagement wird noch in diesem Kapitel genauer eingegangen.

3.2.3 Höhere Gewalt

Versagen der Infrastruktur wie Strom, Wasser oder Telekommunikation führt in der Regel zu gravierenden Ausfällen, da man eine geringe Eintrittswahrscheinlichkeit annimmt und Ausfallssysteme sehr teuer sind und daher oft nicht beschafft werden. Zu höherer Gewalt zählt unter anderem Blitzeinschlag, Feuer, Hochwasser und Überschwemmungen oder Sturm, aber auch Personalausfall herbeigeführt durch Krankheit, Unfall oder Streik.
Um eine Schadensminderung bei höherer Gewalt anzustreben sind Versicherungen sinnvoll. Auch ist die Ausarbeitung von Notfallplänen, welche den Betrieb bei Ausfall des IT Systems weiterlaufen lassen angeraten.

3.2.4 Betrug und Diebstahl

Computerhardware und –software sind wie andere Wertgegenstände Ziele von Diebstählen. Besonders problematisch sind kleine portable Geräte wie Notebooks und PDAs. Aber auch fixes Equipment wie Flachbildschirme oder PCs werden gestohlen. Einerseits kann dies professionell zum Weiterverkauf und somit Geldbeschaffung geschehen oder zur Eigennutzung. Klein- und Verbrauchsmaterial ist durch Diebstahl von Mitarbeitern am meisten betroffen, hier fehlt oft das Bewusstsein eines echten Vergehens. Relevant sind z.B. bereits eingesetzte Datenträger (Disketten, Festplatten) welche von Mitarbeitern weiterverwendet anstatt vernichtet werden, dadurch aber Firmendaten aus dem Unternehmen entwenden.
Software und Datendiebstahl stellt eine Besonderheit dar, es handelt sich meist um ein Kopieren der Daten, welche dann weiterbenutzt werden. Es kann sich dabei um Musik, Videos, Fotos, Software oder andere elektronische Daten handeln. Um mittels eines Computer Systems zu betrügen, werden oft automatisierte Methoden verwendet, also etwas wozu sich Computer selbst hervorragend eignen.

3.2.5 Sabotage

Sabotage, also das absichtliche Herbeiführen von Schaden kann sowohl innerhalb eines Unternehmens geschehen als auch von außen einwirken. Im IT Bereich sind Sabotageakte zum Großteil innerhalb eines Unternehmens anzutreffen, sie werden meist von enttäuschten

Mitarbeitern ausgeführt. Viele Mitarbeiter wissen genau wo sie ein Unternehmen empfindlich treffen können und durch welche Aktionen Abläufe stark gestört werden.

Dazu zählen unter anderem folgende Beispiele:

- Zerstörung von Hardware
- Einbauen von fehlerhaftem Code, welcher zu einem gewissen Zeitpunkt Schaden verursacht
- Eingabe von falschen Daten, Löschen oder Verändern von Daten

Der Anteil an Bedrohungen von Innen ist in den letzten Jahren stark angestiegen und dieser Trend hält an. Mittlerweile wird davon ausgegangen dass 70% der Angriffe von innerhalb eines Unternehmensnetzwerkes ausgehen.[7] Angriffe von intern sind einfacher durchzuführen, da die nach außen wirksamen Schutzmechanismen nicht wirksam sind sobald man Zugriff auf das interne Netzwerk besitzt. Weiters wird meist nur restriktiv eingehender Netzwerkverkehr geblockt, jedoch ausgehende Netzwerkzugriffe generell erlaubt.

3.2.6 Hacker

Dieser Begriff hat mehrere Bedeutungen und ist nicht genau spezifiziert. Er bezeichnet allgemein Personen welche über sehr gutes Computerwissen verfügen und damit IT-Sicherheitssysteme – sowohl Software als auch Hardware – zu umgehen versuchen oder Sicherheitslücken aufdecken. Früher wurde der Begriff Hacker hauptsächlich für herausragende Programmierer verwendet, mittlerweile haftet ihm aber eine negative Bedeutung an, da vor allem in den Medien „**Hacker**“ für kriminelle Computerbenützer verwendet wird. Die Abgrenzung ist jedoch schwierig, da bereits der erfolgreiche Versuch in ein System einzudringen ohne absichtlichen Schaden anrichten zu wollen eine kriminelle Handlung darstellen kann, oder unbewusst das IT-System beeinträchtigen könnte. Für Personen welche absichtlich durch ihre Handlung Systeme beeinträchtigen oder Schaden anrichten wollen wird der Begriff „**Cracker**“ verwendet, sie sind also Hacker mit krimineller

[7] Basierend auf Vulnerability-Scans von Qualys, vorgestellt von Dr. Eschelbeck am Security Forum 2004 in Hagenberg.

Absicht. Ziel von Crackern ist es oft Webseiteninhalte zu verändern, Denial-of-Service Attacken auf bekannte Firmen durchzuführen oder Daten zu stehlen.
Bis vor einigen Jahren wurden diese Attacken noch relativ einzeln auf ausgewählte Systeme durchgeführt. Sicherheitslücken wurden jedoch immer schneller publik und über das Internet Möglichkeiten zum Ausnutzen der Sicherheitsprobleme verbreitet. Die Zeit vom bekannt werden einer Sicherheitslücke bis zum erscheinen eines solchen Exploits nimmt immer mehr ab. Daraus hat sich eine neue Generation von Personen herausgebildet welche diese Exploits ausnutzt ohne über das eigentliche technische Wissen zu verfügen wie die Sicherheitslücke funktioniert. Diese Personengruppe nennt man „**Skript-Kiddies**“ da sie eben nur fertige Software benützen, meist gegen beliebige Ziele. Skript-Kiddies sind sicher die häufigsten Angreifer, da sie aber über relativ wenig Wissen verfügen und sehr oft dieselben Programme verwenden sind Angriffe relativ leicht abzuwehren. Fehlen entscheidende Patches und sind somit bekannte Sicherheitslücken offen oder ist ein System nicht korrekt durch eine Firewall geschützt reichen oft einige Minuten bis eine Attacke durch ein automatisiertes Programm in das System eingedrungen ist.

3.2.7 Industrie- und Wirtschaftsspionage

Industrie- und Wirtschaftsspionage hat zum Ziel einem Unternehmen entscheidende Vorteile durch das Wissen über andere Unternehmen zu bringen. Diese Informationen können aktuelle Finanzdaten, neue Produkte oder Kundendaten umfassen. Dazu werden Personen mit sehr gutem technischem Wissen engagiert um an diese Daten zu gelangen. Umgehrt werden Daten auch oft mit dem Ziel gestohlen um sie an den meistbietenden zu verkaufen. Diese gezielten Attacken werden meist genau vorbereitet und sind im Vergleich zu Skript-Kiddie Angriffen schwieriger abzuwehren, kommen jedoch nicht so häufig vor. Wichtig ist eine konsequente Umsetzung einer firmenweiten Security Policy um möglichst wenig Angriffspunkte zu bieten.

3.2.8 Bösartiger Code

Der Überbegriff „Bösartiger Code“ oder „Malware“ steht für die verschiedenen Arten von Software welche Schaden anrichten können. Dazu zählen **Viren, Würmer, Spyware** und **Trojaner**.

In Analogie zu biologischen Viren ist ein **Computervirus** ein Programm welches sich an andere Computerprogramme anhängt und Kopien von sich selbst erzeugt. Eine

Schadensfunktion ist dabei nicht immer vorhanden, viele Viren geben lediglich zu einem bestimmten Zeitpunk Nachrichten am Bildschirm aus.

Die Definition des BSI für Computervirus [Bsi05/1] lautet: „*Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)*“

Bei Viren wird zwischen Dateiviren, Boot-Sektor-Viren und Makroviren unterschieden [Schn00]. Zu Beginn gab es fast nur Dateiviren, welche jedoch mit Einführung von Betriebssystemen wie Windows 3.1 rasch dezimiert wurden. Die Verbreitung von Boot-Viren ging mit dem selteneren Einsatz von Disketten zurück. Am meisten sind heute noch Makroviren aktiv, welche sich an Datenfiles anhängen und sich der Skriptsprache des auszuführenden Programms bedienen.

Würmer verbreiten sich im Unterscheid zu Viren selbstständig von einem System zum nächsten. Dabei ist es nicht notwendig dass bestimmte Programme vom Benutzer gestartet werden müssen, der Wurm nutzt einfach die benötigten Programme selbst. So nutzten viele Würmer Email Programme wie Outlook um sich an möglichst viele Empfänger weiterzuschicken. Andere Würmer hingegen versuchen über Sicherheitslücken von Webservern, Dateifreigaben und anderen im Internet verfügbaren Diensten in ein System zu gelangen, nur um von dort wieder andere Systeme zu infizieren.

Trojaner werden Schadprogramme genannt welche vorgeben eine nützliche Software zu sein, in Wirklichkeit jedoch in Hintergrund unerwünschte Tätigkeiten ausführen. Dies kann ein offener Zugang zu dem infizierten Rechnersystem sein („Backdoor“), das Überwachen des Tastaturpuffers zum ausspähen von Passwörtern und Kreditkartennummern oder um den Rechner für weitere Zwecke wie Spamversand zu missbrauchen. Die Bezeichnung Trojaner ergibt sich in Analogie aus der Griechischen Sagenwelt wo Odysseus ein hölzernes Pferd baut und dies mit Soldaten beladen in Troja einschleust um von innen die Tore der Stadt zu öffnen. Trojaner bleiben oft unbemerkt am System und verhalten sich ruhig bis sie weitere Informationen erhalten welche Aktionen sie ausführen sollen. Besonders „hilfreich“ sind Trojaner für verteilte Denial-of-Service Angriffe indem eine genügend große Anzahl von Rechnern infiziert wird und diese automatisch zu einem gewissen Zeitpunkt ein Zielsystem attackieren, wodurch das Zielsystem wegen der Überlast nicht mehr erreichbar ist.

3.2.9 Schutz von persönlichen Daten

Personenbezogene Daten sind für viele Unternehmen sehr hilfreich, um ihre Produkte dem richtigen Zielpublikum zu offerieren. Besonders interessant sind hierbei Adressen, Telefonnummern, Einkommen, Beruf oder persönliche Interessen. Die seit 1995 existierende EU-Richtlinie 95/46/EG des Europäischen Parlaments zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten beschreibt Mindeststandards für den Datenschutz [EURO95]. Leider wird diese Richtlinie sehr oft nicht eingehalten und personenbezogene Daten weitergegeben, verkauft und ohne Zustimmung gespeichert.
Da sich die Seriosität der Betreiber von Internetdiensten nicht nachvollziehen lässt, sollten persönliche Daten immer mit der größten Vorsicht und nur so wenig wie möglich weitergegeben werden. In den Medien tauchen in letzter Zeit vermehrt Meldungen über missbräuchliche Verwendung und Diebstahl von Bankdaten und Kreditkartendaten auf. Dabei versuchen Betrüger über gefälschte Emails an Kontodaten und Passwörter zu gelangen. Es gilt also sicherzustellen, wichtige persönliche Daten wie Kreditkartennummer nur bei vertrauenswürdigen Internet-Dienstanbietern einzugeben.

Dieser Unterpunkt von „Bedrohungen und Gefahren“ wird in der Literatur nicht immer aufgeführt. „Schutz von persönlichen Daten“ ist im eigentlichen Sinne keine „Bedrohung“ oder „Gefahr“. Jedoch kann durch unvorsichtiges Verhalten im Internet heutzutage sehr einfach Information zur Missbräuchlichen Verwendung gesammelt werden. Mitgeführt wird dieser Unterpunkt unter anderem in [Sch00] und [Nist95]. Das BSI dagegen geht im Grundschutzhandbuch nicht genauer darauf ein [Bsi05].

3.3 Zielgruppen

Beim IT-Sicherheitsprozess und der darin enthaltenen Entwicklung und späteren Anwendung von Security Policies ist es unumgänglich, jeweils die richtigen Personen in den richtigen Abteilungen und Positionen anzusprechen. In der Start- und Einführungsphase muss vom Management entsprechende Akzeptanz und positive Überzeugung für die umzusetzenden Maßnahmen ausgehen. Endanwender, welche am meisten von Policies betroffen werden, sollten ebenfalls gut informiert werden. Geschieht dies nicht, können Policies schnell als kompliziertes Regelwerk betrachtet werden, welches die tägliche Arbeit verkompliziert, aber keinen Nutzen bringt.
Deshalb muss also auf den unterschiedlichen Informationsbedarf der einzelnen Zielgruppen

eingegangen werden. Daraus resultierend kann es nicht eine Policy für alle geben, sondern unterschiedliche Ausgaben mit den jeweils relevanten Informationen aus der Sicht der Betroffenen. So würde eine Passwort Policy für Administratoren zeigen, welche Parameter in Serversystemen gesetzt werden müssen, wie eine Sperrung des Kontos nach einer gewissen Anzahl falscher Passworteingaben oder die Mindestlänge des Passwortes. Endanwender hingegen müssen ausreichend über die Wichtigkeit von Passwörtern, sinnvolle Zusammensetzungen, Aufbewahrungs- und Weitergaberichtlinien informiert werden.

Wobei man folgende Rollen unterscheidet:
Administratoren installieren, verwalten und betreuen IT Systeme. Sie haben im Vergleich zu anderen Personen im IT Sicherheitsprozess das detaillierteste technische Wissen im Umgang mit den Systemen.
Benutzer oder **Endanwender** benötigen IT Systeme zur Erledigung ihrer Arbeit. Für sie ist ein benutzerfreundliches und ausfallsicheres System von Vorteil.
IT-Betreuer sind die Ansprechpersonen für Benutzer. Sie lösen einfache Probleme und Benutzeranfragen.
IT-Sicherheitsbeauftragter ist eine dazu ernannte Person, welche für IT-Sicherheit und deren Umsetzung im Unternehmen verantwortlich ist.
Ein **Datenschutzbeauftragter** ist für den korrekten Umgang mit personenbezogenen Daten verantwortlich.
Der **IT-Leiter** ist die Führungsposition der Informationstechnik-Abteilung. Er ist für die informationstechnische Struktur eines Unternehmens verantwortlich.
Der **Vorstand** oder **Geschäftsführer** ist für die Leitung des Unternehmens zuständig. Er entscheidet über Investitionen in IT-Sicherheit und deren Umsetzung.

Diese Rollen lassen sich im Security Policy Entwicklungs- und Umsetzungsprozess zu folgenden Zielgruppen zusammenfassen:

Zielgruppe	Zugehörige Rollen	Aufgabe
Geschäftsführer	Vorstand, Geschäftsführer	Strategische IT-Entscheidungen, Bestellung der IT-Verantwortlichen, Sicherstellung der korrekten IT-Nutzung
IT-Verantwortliche	Administratoren, IT-Betreuer, IT-Sicherheitsbeauftragter,	Planung, Umsetzung und Einhaltung der IT-

	Datenschutzbeauftragter, IT-Leiter	Sicherheitsprozesse, Leitlinien und Konzepte
Mitarbeiter	Benutzer, Endanwender	Korrekter Umgang mit IT, Einhaltung der IT-Sicherheits-Vorgaben

Tabelle 2: Zielgruppen bei der Security Policy Entwicklung und Umsetzung

Für die meisten Unternehmen wird diese Aufteilung in drei Gruppen ausreichen. Eine detailliertere Unterteilung (IT-Leitung und Planung, IT-Betreuer, Unterteilung der Benutzer) macht erst ab einer gewissen Unternehmensgröße Sinn, wenn diese Positionen auch wirklich von mehreren eigenständigen Personen besetzt sind. Hierbei steigt dann auch der Aufwand mit der Anzahl der Unterteilungen stark an. Die Regeln werden komplizierter und müssen öfters angepasst werden. Eine Unterstützung durch passende Software-Werkzeuge zum Erstellen und Dokumentieren von Policies ist dann sicherlich von Nutzen.

Zusätzlich zu den in Kapitel 2.4.2 beschriebenen **Systembezogenen IT Security Policies** ergeben sich nun **Zielgruppenbezogene IT Security Policies,** welche die Systembezogenen Policies verfeinern und auf den jeweiligen Informationsbedarf der Zielgruppen optimieren:

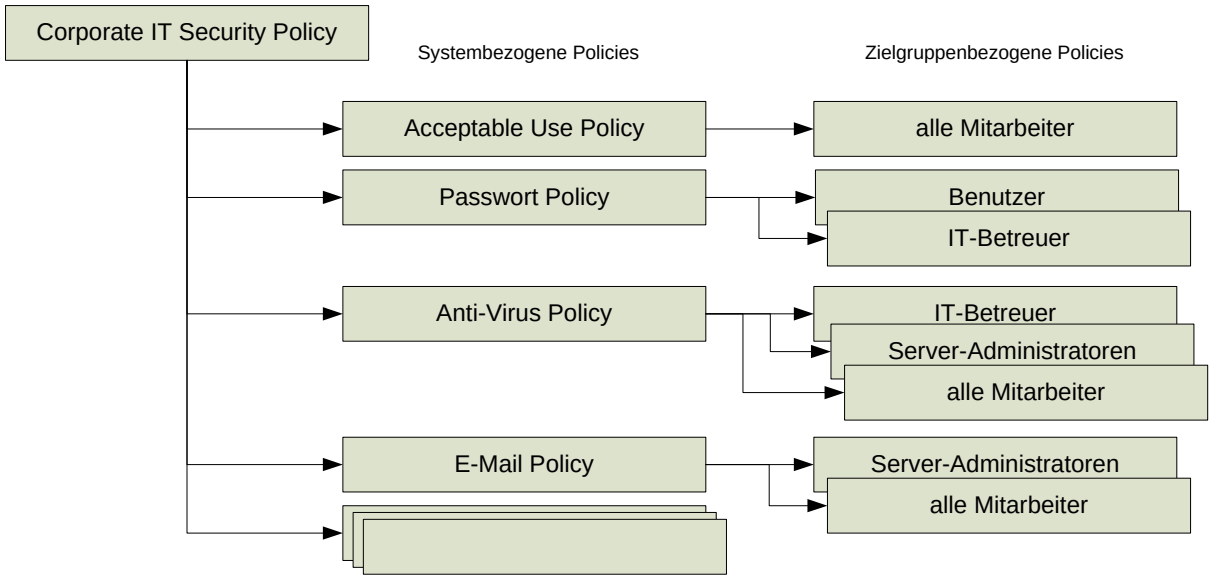


Abbildung 7: Systembezogene und Zielgruppenbezogene Policies

Erst Aufgrund einer solchen Aufteilung können sinnvolle Regeln für unterschiedliche Systeme und unterschiedliche Anwender entstehen. Man merkt, dass schnell eine große Anzahl von Policies nötig sein kann. Dies führt zu einem hohen administrativen Aufwand und

hohen Verwaltungskosten. Bei der Umsetzung sollten deshalb zuerst die wichtigsten Policies entworfen und umgesetzt werden, um somit ein gewisses Maß an Grundsicherheit zu gewährleisten. In einem weiteren Zyklus können diese Policies dann verfeinert und die Sicherheit im Detail nochmals verbessert werden.

3.4 Haftung

Durch die steigende Integration von Informationstechnologie in viele Unternehmensprozesse hat sich erst in den letzten Jahren die Problematik der Haftung bezüglich korrekten Einsatzes von Informationstechnologie ergeben. Nicht nur IT Unternehmen sind vom reibungslosen Funktionieren ihrer IT-Infrastruktur abhängig, fast alle Betriebe in vielen Branchen stützen ihre Arbeitsabläufe durch den Einsatz von Hard- und Software.
Daraus sind im Bereich der IT-Sicherheit Haftungsgrundsätze entstanden welche das Unternehmen oder Mitarbeiter treffen.

Zur besseren Anschaulichkeit folgen einige Beispiele über verschiedene Szenarien der Haftung im IT-Sicherheitsbereich. Die Beispiele a) und c) stammen aus persönlicher Erfahrung im Bereich IT Outsourcing, b) und d) sind Gedankenmodelle aus IT-Security Projekten.

a) Unternehmen A hat zum Datenaustausch sein Netzwerk mit einem Partner B verbunden. Die zwei Unternehmen vertrauen einander und sichern die Verbindung nur nach außen gegen Dritte ab. Durch fehlenden Einsatz eines Anti-Virus Produktes wird Unternehmen A von einem Computervirus befallen, welcher sich über die offene Verbindung zu Unternehme B ausbreitet und erheblichen Schaden verursacht.

b) Der Webserver eines Unternehmens wurde durch fehlerhafte Konfiguration der Firewall von einem Angreifer kompromittiert und die Inhalte verändert. Zum Absichern von im Internet verfügbaren Diensten war eine Security Policy vorhanden, welche bei korrekter Umsetzung das Problem verhindert hätte.

c) Eine wichtige produktive Datenbank ist auf einem fünf Jahre alten Datenbankserver in Verwendung. Dieser läuft seit einem halben Jahr nicht mehr stabil, was auf einen Hardwaredefekt schließen lässt. Support vom Hersteller des Servers ist nicht mehr

möglich. Das Problem wurde vom IT-Verantwortlichen der Geschäftsleitung mitgeteilt, jedoch wurden keine Mittel zur Neuanschaffung genehmigt.

d) Bei einem Brand in einem kleineren Produktionsunternehmen werden Teile des Serverraums zerstört, die Produktion muss bis zur Wiederherstellung der IT stoppen. Dies gelingt innerhalb von 4 Tagen durch extern gelagerte Backups und neu angeschaffte Hardware, trotzdem entsteht beträchtlicher Umsatzverlust.

Mittlerweile wird davon ausgegangen, dass Sicherheit dem Stand der Technik entsprechen muss und dabei aber wirtschaftlich durchführbar bleiben soll. In Fall a) hätte das Unternehmen A zumindest ein Anti-Virus Produkt einsetzen müssen, keines zu verwenden gilt heutzutage als grob fahrlässig. Für Schäden, die aus solcher Fahrlässigkeit entstehen, haften die Unternehmen.
Fall b) lässt auf eine leichte oder mittlere Fahrlässigkeit des verantwortlichen Dienstnehmers schließen da vorhandene Richtlinien nicht eingehalten wurden. Solange dies keine vorsätzliche Handlung ist und nicht regelmäßig auftritt haftet der Dienstnehmer nicht.
Im Fall c) war der Geschäftsleitung das Problem bekannt, sie hat aber nicht reagiert. Da die Geschäftsleitung für die Sicherstellung einer bedarfskonformen IT-Nutzung verantwortlich ist, haftet sie auch für Unternehmensverluste durch Ausfall der Systeme.
Im Gegensatz dazu gibt es im letzten Beispiel keine direkte Haftung. Es wurden adäquate Vorkehrungen für einen Katastrophenfall getroffen. Die Anschaffung eines Ersatzrechenzentrums hätten den Ausfall zwar verhindert, wäre aber nicht angemessen und wirtschaftlich für ein kleines Unternehmen nicht tragbar. (Da es sehr kostenintensiv und teilweise unmöglich ist für Katastrophenfälle wie Feuer- oder Wasserschäden Sicherheitsvorkehrungen zu treffen, diese jedoch sehr selten auftreten, kann eine Risikominimierung unter anderem durch Versicherungen erreicht werden.)

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) gibt in seinem Leitfaden „Matrix der Haftungsrisiken“ [Bit05] einen guten Überblick über Haftung im IT-Sicherheitsbereich, wobei folgende Aufgabenbereiche unterschieden werden [Bit05, S. 5, gekürzt]:

„Strategische Aufgaben

1. Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung

2. Bestellung eines betrieblichen Datenschutzbeauftragten

Konzeptionelle Aufgaben

1. Einführung eines Sicherheitskonzepts (inkl. Katastrophen- und Zugriffsschutz) und eines Datenschutzkonzeptes

2. Ständige Aktualisierung des Sicherheits-/Datenschutzkonzeptes

3. Regelungen beim Zugang von externen Dritten zu Datenverarbeitungssystemen

4. Professionelle Beschaffung von IT-Systemen und Durchführung von IT-Projekten

5. Sicherung von Vertraulichkeit und Geheimhaltung

Operative Aufgaben

1. Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung

2. Datenschutzrechtliche Konformität sicherstellen

3. Einsatz von SPAM- und Viren-Filtern abwägen

4. Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz

5. Verhinderung von Schädigung Dritter durch firmeneigene IT insbesondere Virenfreier Daten-/Datenträgeraustausch

6. Durchführung regelmäßiger Backups

7. Verwendung lizenzierter Software

8. Einhaltung der Urheberrechte“

Österreichische Gesetzte zu diesem Thema können im Rechtsinformationssystem des Bundes [Ris05] nachgelesen werden:

> Datenschutzgesetz 2000: Bundesgesetz über den Schutz personenbezogener Daten
> E-Commerce Gesetz: Regelung bestimmter rechtlicher Aspekte des elektronischen Geschäfts- und Rechtsverkehrs
> StGB § 118a: Widerrechtlicher Zugriff auf ein Computersystem
> StGB § 119a: Missbräuchliches Abfangen von Daten
> StGB § 126a: Datenbeschädigung
> StGB § 126b: Störung der Funktionsfähigkeit eines Computersystems
> StGB $ 126c: Missbrauch von Computerprogrammen oder Zugangsdaten

Unternehmen müssen ein IT-Risikomanagement durchführen und nach dem momentan aktuellen Stand der Technik arbeiten. Dabei können Security Policies als Schnittstelle zwischen der Unternehmensleitung, den IT-Verantwortlichen und Mitarbeitern eingesetzt

werden. Security Policies gelten dabei für Mitarbeiter als Richtlinie, was für sie erlaubt ist und wie der Umgang mit der IT zu erfolgen hat.

3.5 Kostenfaktor

Bei der Verbesserung der IT Sicherheit sind meist die Kosten ein ausschlaggebender Faktor, ob Maßnahmen umgesetzt werden oder nicht. Oft ist es schwierig diese zusätzlichen Kosten zu rechtfertigen, da meist nicht genau beziffert werden kann, welche möglichen spekulativen Kosten durch sicherheitsrelevante Schadensfälle entstehen können.
Genau dies kann jedoch zur Motivation dienen, IT Security Policies zu erstellen: Die Verringerung von IT-Risiko durch geeignete kostenadäquate Maßnahmen.

Wie viel muss man in IT Sicherheit investieren?

Diese entscheidende Frage hat jedes Unternehmen für sich zu beantworten, es gibt keine generelle Lösung. Ohne Investitionen wird sich die IT Infrastruktur in einem unsicheren Zustand auf geringem Verfügbarkeitsniveau befinden. Ab einem gewissen Punkt jedoch stehen die Kosten in keinem Verhältnis mehr zum dadurch verringerten Risiko. Es gilt einen Punkt in der Mitte zu finden, welcher das Risiko auf ein erträgliches Maß minimiert und von den Investitionen noch vertretbar ist. Dabei spielen viele Faktoren wie Unternehmensgröße, Branche, Gesetze oder Verträge eine Rolle.

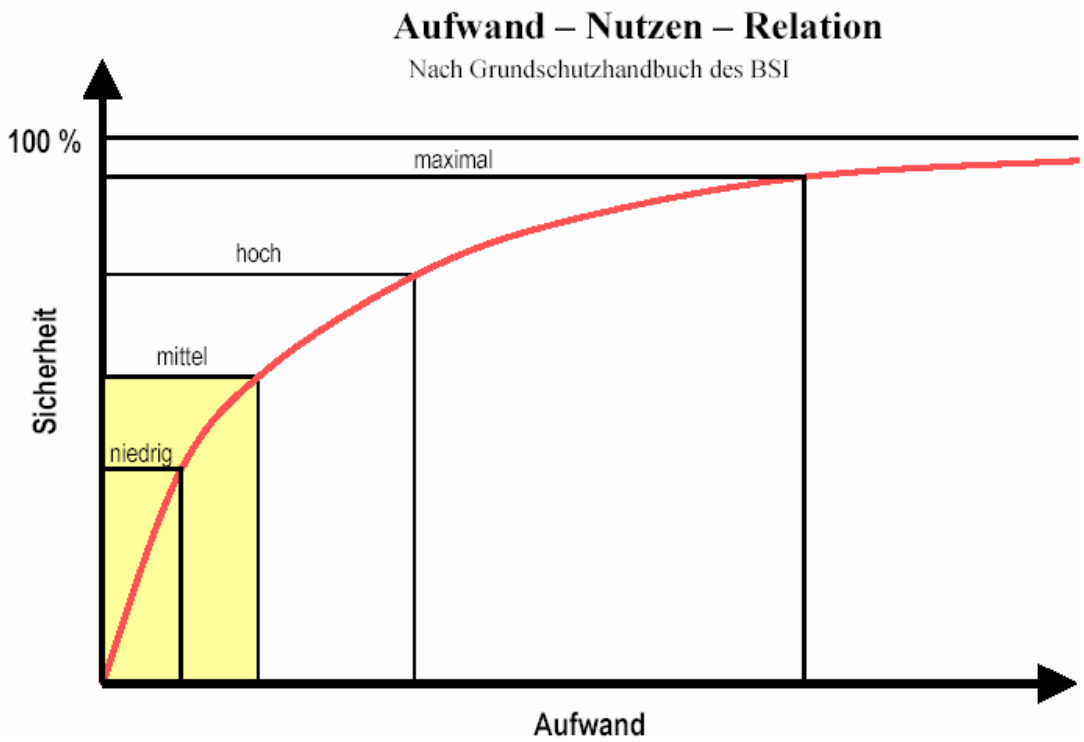


Abbildung 8: Aufwand-Nutzen-Relation

Wie aus der Abbildung ersichtlich ist, kann eine hundertprozentige Sicherheit nicht erreicht werden. Dies liegt daran, dass nicht alle Ereignisse bekannt sein können, welche die Sicherheit beeinträchtigen und somit ein potentielles Risiko bedeuten. Dazu zählen zum Beispiel nicht bekannte Sicherheitslücken, vor welchen man sich natürlich auch noch nicht schützen kann. Da der Aufwand im Verhältnis zur erreichten Sicherheit proportional immer größer wird, ist es noch relativ einfach ein geringes Sicherheitsniveau zu erreichen, auch die dabei entstehenden Kosten sind überschaubar. Als Ansatz dafür reicht meist der Einsatz einer gut konfigurierten Firewall, ein aktueller, durchgängiger Viren- und Spywareschutz und ein ordentliches Backup Konzept.

Leider wird klassischerweise erst in IT Sicherheit investiert, wenn durch einen Sicherheitsvorfall Systeme nicht verfügbar sind und dadurch Kosten, Image- oder Umsatzverluste entstehen. Ausgaben im IT Sicherheitsbereich lassen sich sehr schlecht mit dem Return On Investment (ROI) rechtfertigen, da kein Gewinn durch den Einsatz von Kapital im Sicherheitsbereich entsteht, sondern „nur“ Verluste durch geringere Ausfälle vermieden werden. Diese Verluste lassen sich aber nur schwer in Zahlen fassen, da sie nur mit einer gewissen Wahrscheinlichkeit auftreten. Eine bessere Möglichkeit Ausgaben zu rechtfertigen ist deshalb ein gutes Risikomanagement. Dabei wird der potentielle Schaden der

Ausfallswahrscheinlichkeit gegenübergestellt, wodurch abgeschätzt werden kann, welche Risiken zu hoch sind und welche Risiken in Kauf genommen werden.
In einer Studie der InformationWeek [InfW04] im Jahr 2004 wurde unter anderem gefragt wie IT Sicherheitsinvestitionen gerechtfertigt werden. Dabei wurden 842 Antworten von IT-Managern und Sicherheitsverantwortlichen zu über vierzig Fragen aus allen Bereichen der Informationssicherheit ausgewertet.

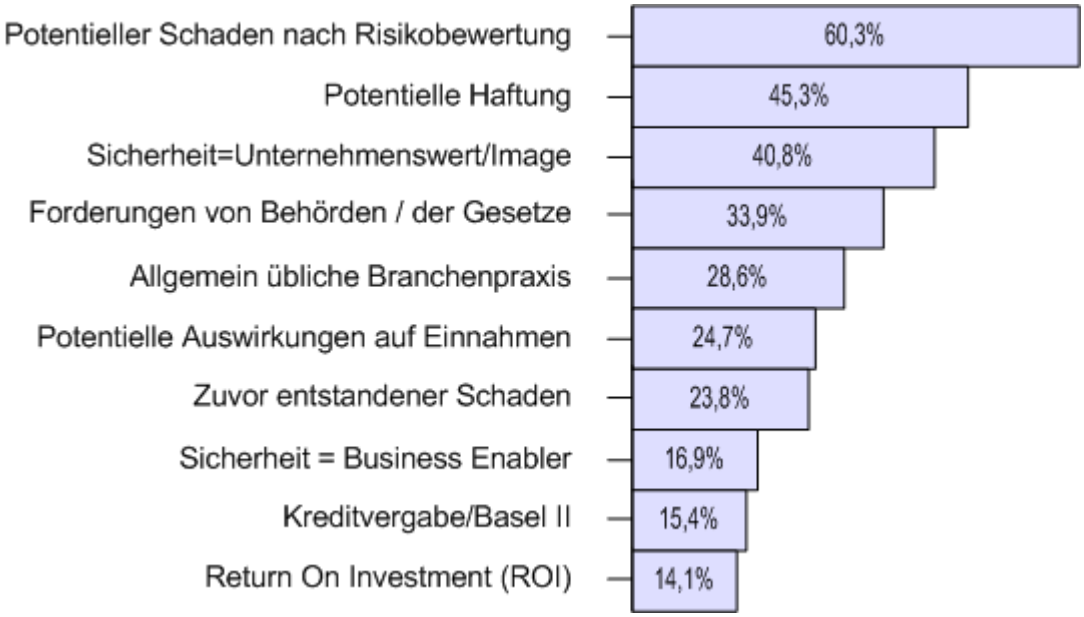


Abbildung 9: Wie werden Sicherheitsinvestitionen gerechtfertigt [InfW04]

Dabei wurden die Risikobewertung, Haftung, und Sicherheit als Unternehmenswert am meisten als Rechtfertigungsgrund genannt. Den Schluss bildet der ROI, der wie erwähnt bei Investitionen im Sicherheitsbereich keine oder nur eine sehr geringe Aussagekraft besitzt. Es liegt also Nahe als erstes mit einer groben Risikobewertung einen Sicherheitsprozess zu beginnen und sich ebenfalls über die Haftungsrisiken einen Überblick zu schaffen.

Wirtschaftlichkeit

Investitionen in IT Sicherheit müssen natürlich auch wirtschaftlich sein. Dabei kann man grundsätzlich folgende Methoden zur Bewertung anwenden [Pohl04]:

„Nach Kostenaspekten

- ***Total Cost of Ownership***
  - *Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und IT-Sicherheitsmaßnahmen*
  - *Entspricht der Kapitalwert-Methode*
    (Was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen?)

Nach Nutzenaspekten

- *ROI = Return on Investments*
- *Nutzen den Kosten gegenübergestellt*
  (Was nützt ein Investment bezüglich Kostenminimierung und/oder Umsatzsteigerung, wann hat sich eine Investition amortisiert, d.h. die Anschaffungskosten für eine Investition werden durch den mit der Investition erwirtschafteten Ertrag gedeckt? Je schneller eine Deckung erzielt wird, umso schneller kann ein Gewinn, z.B. durch das Investment in IT-Sicherheitsmaßnahmen, generiert werden.)“

Investitionen müssen meist gerechtfertigt werden, was dazu führt, dass eine Kosten/Nutzen-Gegenüberstellung wohl die häufigste Entscheidungsgrundlage ist. Gerade der Nachweis des Nutzens einer besseren IT-Sicherheit ist schwer zu erbringen. Deshalb ist es sinnvoll, IT-Sicherheit mit Risikomanagement in Verbindung zu bringen. Ohne ausreichende IT-Sicherheitssysteme ist das Risiko für mögliche Schäden hoch, erst Sicherheitsinvestitionen senken das potentielle Risiko eines Schadens.

Abbildung 10: IT Sicherheitsrisiken und Investitionen, zeigt den Zusammenhang zwischen den Kosten durch mögliche Schäden und Sicherheitsinvestitionen in Bezug auf die getätigten Sicherheitsmaßnahmen. Dabei ist wieder ersichtlich, dass die größte Risikominimierung durch die als erstes getätigten Maßnahmen erzielt wird. Umso sicherer ein System gemacht werden soll, umso höher steigen auch die Kosten, und zwar überproportional im Vergleich zu den verminderten Risiken.

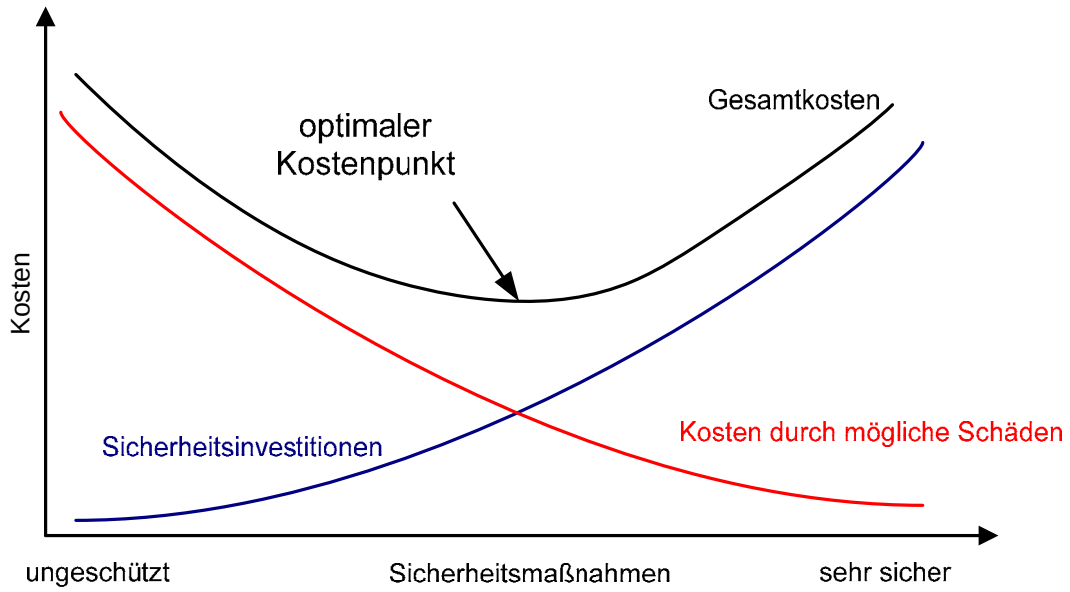


Abbildung 10: IT Sicherheitsrisiken und Investitionen

Der ersichtliche wirtschaftlich optimale Kostenpunkt ergibt sich aus der Summe der Sicherheitsinvestitionen und den verbleibenden Kosten durch mögliche Schäden. Es ist aber nicht Ziel eines jeden Unternehmens, diesen Punkt zu erreichen Viele Unternehmen geben sich mit weniger Sicherheit zufrieden und nehmen die höheren Risiken in Kauf. Besonders bei kleinen und mittleren Unternehmen ist dies der Fall. Mit der Größe des Unternehmens steigen meist auch der Sicherheitsbedarf und damit die Investitionen. Wenn die Wirtschaftlichkeit von IT-Investitionen eine untergeordnete Rolle spielt gelangen Unternehmen in den Bereich, wo die Gesamtkosten wieder steigen. Dies kann durch gesetzliche Vorgaben wie im Gesundheitswesen oder im militärischen Bereich nötig sein. Auch in Unternehmensbranchen wie dem Finanzwesen ist es aus Imagegründen wichtiger, Risiken möglichst zu minimieren, fast unabhängig von den Kosten.

Eine vollkommene, hundertprozentige Sicherheit ist aber nicht zu erreichen. Dies würde bedeuten, dass absolut kein Ausfall möglich ist – alleine die Fehlerfreiheit von Software kann nicht bewiesen werden, ebenso wie die Korrektheit eines Prozessordesigns.

Eventuelle Schäden durch Restrisiken können am besten durch Versicherungen abgedeckt werden. So kann zum Beispiel eine Brand- oder Katastrophenversicherung den Schaden bei Komplettausfall einer IT-Infrastruktur ausgleichen. Eine technische Lösung wäre ein komplettes redundantes Rechenzentrum, welches natürlich ein Mehrfaches an Kosten verursachen würde.

3.6 Prozessmodelle

3.6.1 IT-Sicherheitsmanagement nach österreichischem IT-Sicherheitshandbuch

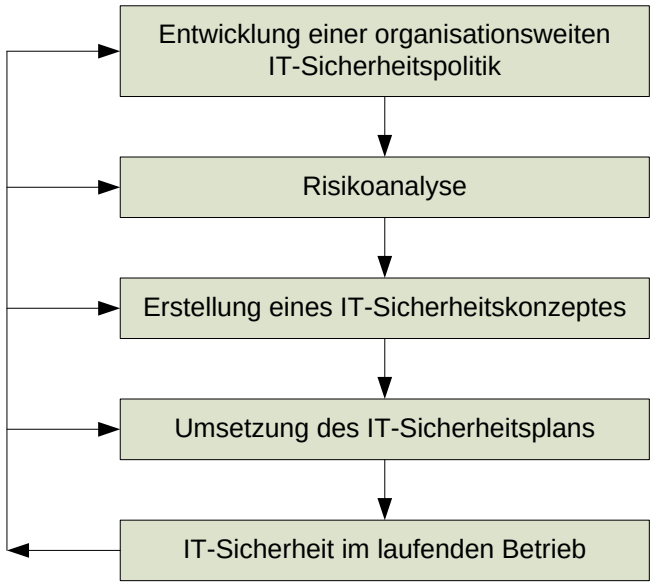


Abbildung 11: Übersicht der Aktivitäten im IT-Sicherheitsmanagement nach IT-Sicherheitshandbuch [Sihb04]

„Abbildung 11: Übersicht der Aktivitäten im IT-Sicherheitsmanagement nach IT-Sicherheitshandbuch“ zeigt die zentralen Aktivitäten im IT-Sicherheitsmanagementprozess nach österreichischem IT-Sicherheitshandbuch. Dabei steht die **Entwicklung einer organisationsweiten IT-Sicherheitspolitik**, welche auch als Corporate IT Security Policy bezeichnet wird, an erster Stelle und ist somit der auslösende Schritt des Prozesses. Der Prozess basiert insbesondere auf den "Guidelines on the Management of IT Security (GMITS), ISO/IEC 13335“ [Sihb04, S. 10]

Aufgrund der organisationsweiten IT-Sicherheitspolitik wird eine **Risikoanalyse** durchgeführt um Risiken aufzuzeigen und sie auf ein akzeptables Maß zu reduzieren. Dabei können verschiedene Methoden wie die **detaillierte Risikoanalyse,** der **Grundschutzansatz** oder der **kombinierte Ansatz** angewendet werden.

Auf Basis der Ergebnisse der Risikoanalyse können Maßnahmen ausgewählt werden, um die Reduktion der Risiken auf das gewünschte Maß zu erreichen. Dies geschieht im Rahmen der **Erstellung des IT-Sicherheitskonzeptes**. Bei der anschließenden **Umsetzung des IT-Sicherheitsplanes** sollte besonders auf einen gut strukturierten und genau dokumentierten

Ablauf geachtet werden. Abschließend muss die implementierte Sicherheit auch im laufenden Betrieb aufrechterhalten und gegebenenfalls angepasst werden.

3.6.2 IT-Sicherheitsprozess nach deutschem Grundschutzhandbuch

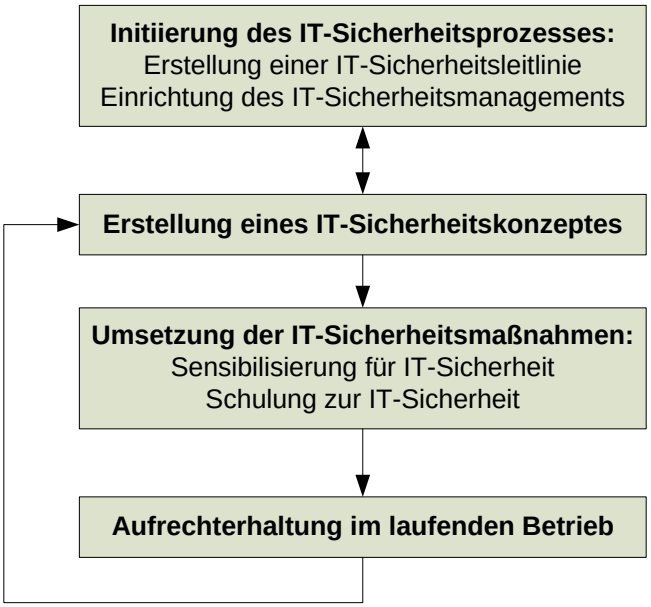


Abbildung 12: IT-Sicherheitsprozess nach IT-Grundschutzhandbuch [Bsi05]

Der Prozessablauf im deutschen Grundschutzhandbuch, welches als Vorlage für das österreichische Sicherheitshandbuch diente, ist sehr ähnlich aufgebaut. Ebenfalls wird die **Initiierung des IT-Sicherheitsprozesses** mit der Erstellung einer IT-Sicherheitsleitlinie begonnen. Weiters zählt dazu auch die Definition der Sicherheitsziele und die Einrichtung eines IT-Sicherheitsmanagements.

Bei der **Erstellung des IT-Sicherheitskonzeptes** werden Schwachstellen identifiziert um geeignete Maßnahmen auswählen zu können. Hierzu können die IT-Grundschutzerhebung, eine Risikoanalyse, eine Schwachstellenanalyse für ausgewählte Bereiche oder Penetrationtests eingesetzt werden.

Das Sicherheitsmanagement ist weiters verantwortlich für die **Umsetzung der Maßnahmen** in den Bereichen Infrastruktur, Organisation, Personal, Technik, Kommunikation und Notfallvorsorge sowie Sensibilisierung und Schulung.

Mit der **Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb** kehrt der Prozess wieder zur Erstellung des Sicherheitskonzeptes zurück, womit sich der Prozessablauf schließt.

3.6.3 Makosi Modell

Das Ziel des MakoSi (Management komplexer Sicherheitsmechanismen) Projektes ist die Entwicklung von Softwarewerkzeugen, die den Prozess der Erstellung von Security Policies für Kooperationsszenarien von der Formulierung der Anforderungen bis hin zur Konfiguration der IT-Infrastruktur unterstützen [Mak03].
Entwickelt wurde das Modell von Projektpartnern an der technischen Universität Darmstadt und verschiedenen Fraunhofer Instituten.
Das Modell geht davon aus, dass Unternehmen ihre Sicherheitsanforderungen in Form von Security Policies spezifiziert, welche für das ganze Unternehmen, Unternehmensteile oder Kooperationen gelten. Ziel des Vorgehensmodells ist es, domänenübergreifende Zusammenarbeit zu realisieren und die beteiligten Stakeholder von der Spezifikation bis zur Implementierung zu unterstützen.

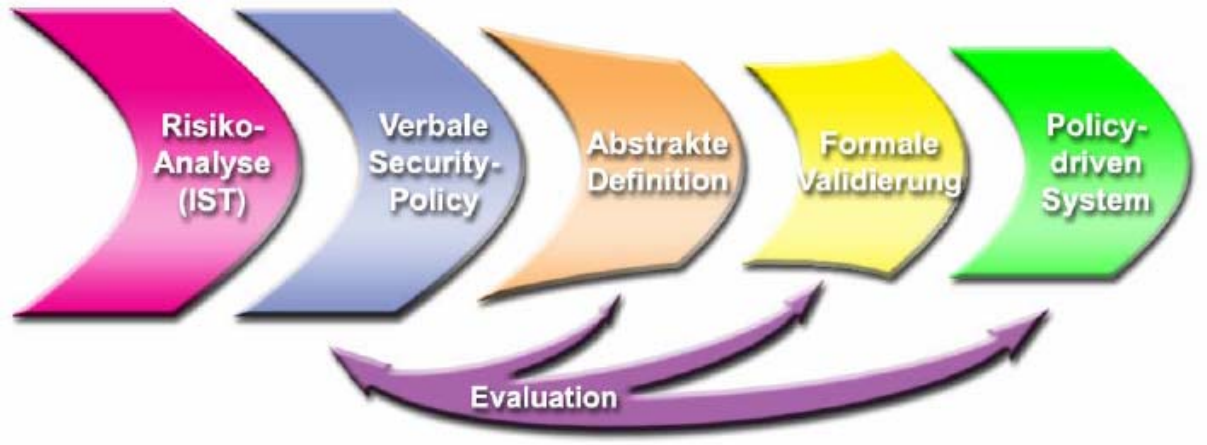


Abbildung 13: Meilensteine des Makosi-Vorgehensmodells [Mak03/2]

Eine Domäne, im Makosi Modell auch Security Policy Domain genannt, ist dabei eine Unterteilung um Ressourcen und Anwender bestimmten Gruppen mit ähnlichen Sicherheitsanforderungen zuzuordnen.

Wie beim SANS Institute oder CERT Coordination Center werden Security Policies im Makosi Modell als einzelne Dokumente zu bestimmten Anwendungsklassen betrachtet, und nicht als ein großes Dokument gesehen. So können Policies auf Security Policy Domains oder Stakeholder abgestimmt werden.

Bevor eine abstrakte Definition der Policies erfolgt, werden diese verbal beschrieben – dies entspricht in etwa dem Prozessabschnitt „Erstellung des IT-Sicherheitskonzeptes“ aus dem deutschen Grundschutzhandbuch. Dabei schlägt das Makosi-Modell folgenden Weg zur Spezifikation von Sicherheitsrichtlinien vor:

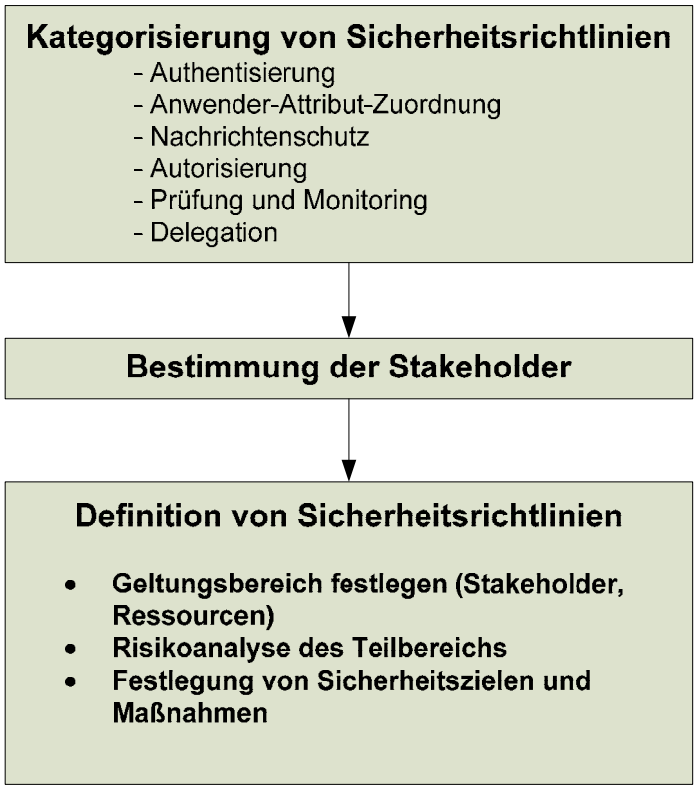


Abbildung 14: Spezifikation verbal beschriebener Sicherheitsrichtlinien, zusammengefasst aus [Mak03/2, S. 1-4]

Zu Beginn steht die **Kategorisierung anhand der Sicherheitsmechanismen** [HFBK03]:

- Authentisierung – Definition der Authentisierungsprotokolle
- Anwender-Attribut-Zuordnung – Festlegung, über welche Sicherheitsattribute ein authentifizierte Anwender zu verfügen hat
- Nachrichtenschutz – Definition von Maßnahmen zum Schutz auszutauschender Geschäftsdaten, d. h. Authentizität, Vertraulichkeit, Integrität etc.
- Autorisierung – Definition, welche Anwender bzw. Anwendungen welche Zugriffrechte auf Ressourcen in der verteilten Umgebung haben

- Prüfung und Monitoring – Festlegung, welche Events zu protokollieren sind

- Delegation – Festlegung, ob und wie Benutzerprivilegien an Systeme weitergereicht bzw. vererbt werden.

- Als nächstes werden die **Stakeholder bestimmt**, also wer für die entsprechenden Sicherheitsrichtlinien zuständig ist. Empfohlen wird, dass dies die jeweiligen Owner (Geschäftsdaten-Owner, System-Owner) und Anwender sein sollen. Diese legen das geforderte Sicherheitsniveau aufgrund ihrer Anforderungen fest.
  Erst danach werden die **Sicherheitsrichtlinien definiert**. Dabei wird besonders darauf hingewiesen, dass alle verwendeten Begrifflichkeiten genau und einheitlich bestimmt sein müssen, um Ungenauigkeiten und Fehler zu vermeiden. Dabei gibt das Makosi-Modell keine Hilfestellung, wie Sicherheitsziele und Maßnahmen festgelegt werden sollen, oder genauerer Beispiele. Es soll jedoch unter anderem besonders auf folgende Punkte geachtet werden:

  - Angestrebtes Sicherheitsniveau
  - Beschaffungskosten
  - Administrations- und Wartungsaufwand
  - Benutzerfreundlichkeit
  - Skalierbarkeit
  - Investitionssicherheit

Ab diesem Prozessabschnitt unterscheidet sich das Makosi-Modell grundlegend vom Sicherheitshandbuch und Grundschutzhandbuch. Das Makosi-Modell geht im weiterführenden Prozess auf die reine Abstrakte Darstellung der Sicherheitsrichtlinien in Form von Zustandsmodellen ein und bildet diese grafisch und mit Hilfe von Tools ab, während die anderen Handbücher Maßnahmenkataloge und deren Umsetzung anführen.

3.6.4 Gemeinsamkeiten der Modelle

Die grundlegenden Gemeinsamkeiten der beschriebenen Modelle können durch den **Deming-Kreis** leicht erkannt werden. Das Management Gedankenmodell Deming-Kreis wurde von William Edwards Deming Mitte des 20. Jahrhunderts entwickelt und ist heute in vielen Qualitätsmanagementsystemen enthalten. Es basiert auf den vier Phasen Plan-Do-Check-Act welche sich kontinuierlich wiederholen und somit einen permanenten Kontrollprozess bilden [Dem05].

Sowohl das IT-Sicherheitshandbuch als auch das Grundschutzhandbuch können als Ausgangspunkt für einen solchen PDCA-Zyklus gesehen werden. Sie bilden die einzelnen Phasen von der Risikoanalyse über die Maßnahmen zur Überwachung und Restrisiko bis zur Aufrechterhaltung im laufenden Betrieb genau ab.

Im BS 7799-2 wird aufgrund des PDCA-Zyklus eine Erhöhung des Informations-sicherheitsniveaus angestrebt. Im Unterschied zu den Sicherheitshandbüchern liegt beim BS 7799-2 der Fokus auf die stetige Verbesserung des durchlaufenen Zyklus. Aufgrund des BS 7799-2 wurde beim Makosi-Modell der Deming-Kreis zur Definition von Security-Policies verwendet, mit besonderem Bezug auf die Plan Phase.

Abbildung 15: Deming-Kreis nach BS7799-2 aus [Mak03/2]

In der Literatur wird öfters der **Security Policy Lifecycle** beschrieben. Dieser umfasst die Phasen **Policy, Enforcement (Durchführung)** und **Assurance (**Qualitätskontrolle, Optimierung):

Policy: In dieser Ermittlungsphase erfolgt die Identifizierung der möglichen Risiken und Bestimmung der zu schützenden Objekte. Aufgrund dieser Analyse werden Maßnahmen (Security Policies) entwickelt und deren Umsetzung geplant.

Enforcement: Hier wird zuerst die Policy und deren Durchführbarkeit getestet und nach positivem Test umgesetzt. Hierzu zählen alle Maßnahmen wie Sicherheitseinstellungen, Benutzerschulungen, Policy Veröffentlichungen oder Konsequenzen bei Verstoß gegen Policies.

Assurance: In dieser Kontrollphase wird die Policy, deren Strategie und Wirksamkeit überprüft. Notwendige Korrekturen fließen in den nächsten Policy Lifecycle zur Anpassung ein.

Abbildung 16: Security Policy Lifecycle aus [Fail99]

Auch diese Prozessdarstellung lässt sich auf den Deming-Kreis zurückführen. Hierbei entspricht die „Policy“ Phase des Security Policy Lifecycles der „Plan“ Phase des Deming-Kreises, die „Enforcement“ Phase der „Do“ Phase. Die Lifecycle Phase „Assurance“ kann als Zusammenfassung der „Check/Act“ Phasen gesehen werden.

3.7 Risikomanagement

3.7.1 Ablauf der Risikoanalyse

„Eine wesentliche Voraussetzung für erfolgreiches IT-Sicherheitsmanagement ist die Einschätzung der bestehenden Sicherheitsrisiken. In einer **Risikoanalyse** wird versucht, diese Risiken zu **erkennen** und zu **bewerten** und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.“ [Sihb04, S.29]
Für adäquate IT Security Policies ist das Risikomanagement unumgänglich, da erst durch das Bestimmen der Risiken und Bedrohungen geeignete Maßnahmen entworfen und eingeleitet werden können. Die Risikoanalyse ist eigentlich ein Managementwerkzeug um Entscheidungen begründet treffen zu können. Daher muss die Risikoanalyse immer zu Beginn eines IT-Sicherheitsmanagementprozesses stehen.
Das Ergebnis der Risikoanalyse ist ein Bericht über alle IT-Systeme und Komponenten und deren Schutzbedarf, welcher dem höheren Management als Entscheidungshilfe für Investitionen und Sicherheitsmaßnahmen dient.

Risiko wird dabei definiert als:
Die Möglichkeit (Potential), dass eine gegebene Bedrohung eine Schwachstelle ausnutzt und einen Schaden anrichtet.

Ein Risiko wird charakterisiert durch zwei Faktoren:

- die Wahrscheinlichkeit des Auftretens (Eintrittswahrscheinlichkeit)
- seine Auswirkung (Schadenshöhe)

Somit ergibt sich die Formel
Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe oder **R = E x S**

Eingebettet in den IT-Sicherheitsprozess ergibt sich bei der Risikoanalyse folgender Ablauf:

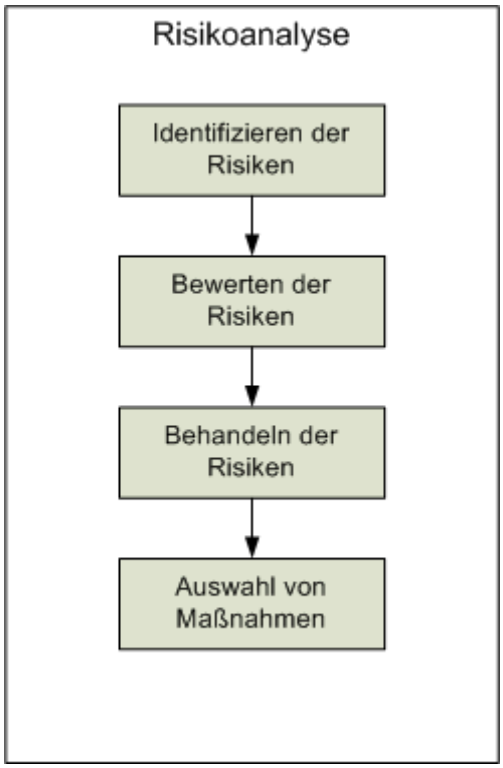


Abbildung 17: Prozessablauf bei der Risikoanalyse, vereinfacht aus [Sihb04]

Im ersten Schritt werden die **Risiken identifiziert,** welche sich durch verschiedene Bedrohungen ergeben. Eine vollständige Aufstellung aller Bedrohungen für alle IT-Systeme wird selten möglich sein, und ist meist auch zu umfangreich. Hilfestellung hierbei geben Gefährdungskataloge wir aus dem Grundschutzhandbuch, welche die wichtigsten Bedrohungsarten klassifizieren und somit eine Zuteilung zu den IT-Systemen einfacher machen.

Beim **Bewerten der Risiken** gibt es mehrere Methoden, die bekanntesten sind die **Detaillierte Risikoanalyse**, der **Grundschutzansatz** und der **kombinierte Ansatz.** Dabei geht es in jeder Methode darum, die Werte des Unternehmens, das Resultat wenn eine Bedrohung eintritt und den damit verbundenen Verlust festzustellen. Dies kann Datenverlust, nicht verfügbare IT-Systeme, unautorisierter Zugriff oder immaterielle Werte wie Imageverlust oder reduziertes Kundenvertrauen sein.

Wenn nun bei der Risikoanalyse die Werte und Gefährdungspotentiale der IT-Systeme bekannt sind müssen die **Risiken behandelt** werden und Entscheidungen hinsichtlich der weiteren Maßnahmen getroffen werden. Dabei gibt es folgende Möglichkeiten:

- **Bedrohungen akzeptieren:** Das Risiko ist bekannt und wird als solches ganzheitlich akzeptiert. Dies kann verschiedenen Ursachen haben wie zu teure Gegenmaßnahmen, geringe Eintrittswahrscheinlichkeit oder sehr geringes Schadenspotential.

- **Bedrohungen verringern:** Das Risiko ist als zu hoch eingestuft und muss verringert werden. Nach der Formel R = E x S kann, um das Risiko zu verringern, entweder die Eintrittswahrscheinlichkeit (z.B. durch ausfallsichere Hardware) oder die entstehende Schadenshöhe (z.B. durch Ersatzhardware und dadurch kürzeren Ausfallzeiten und Hardware-Wartungsverträge) reduziert werden.

- **Versichern gegen die Bedrohung:** Da perfekte, hundertprozentige Sicherheit ohne Restrisiko nicht möglich ist kann es sinnvoll sein, sich gegen Bedrohungen, welche nicht durch wirtschaftlich sinnvolle Maßnahmen abgewandt werden können, zu versichern. Hierzu zählen unter anderem Feuer- und Diebstahlversicherungen oder Betriebsausfallversicherungen.

Folgende Grafik veranschaulicht, wie Risiken durch geeignete Maßnahmen in einen Status gebracht werden in dem sie akzeptiert werden:

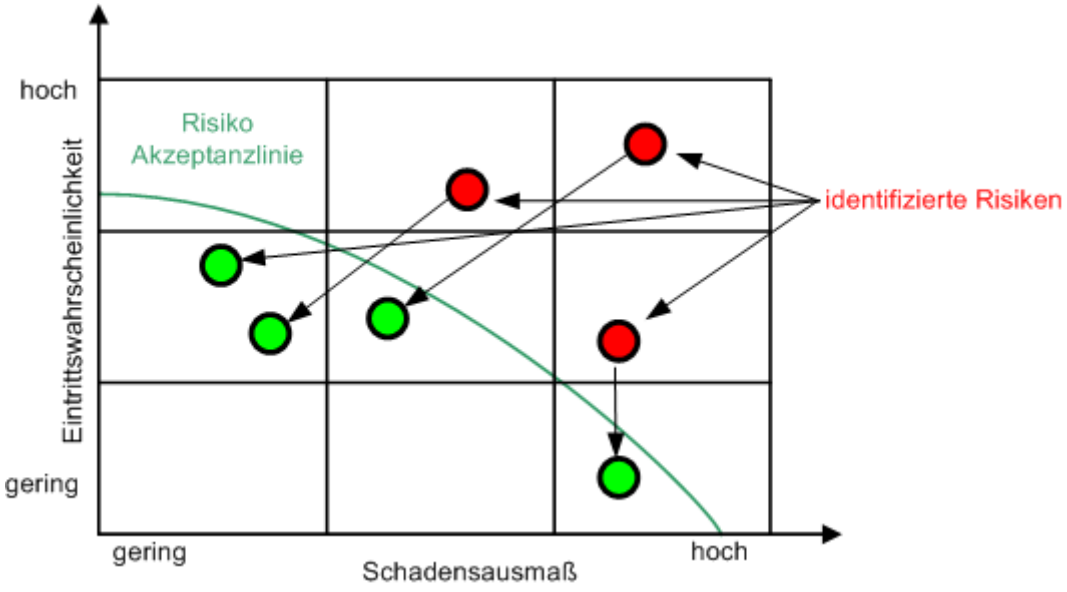


Abbildung 18: Behandlung von Risiken

Für die Risikoanalyse ist es wichtig, sich auf eine Strategie festzulegen. Die Auswahl der Strategie hängt unter anderem von der Unternehmensgröße, dem Budget, Zeitrahmen der Risikoanalyse und gewünschtem Detaillierungsgrad ab.

3.7.2 Detaillierte Risikoanalyse

Hier wird für alle IT-Systeme eine detaillierte Risikoanalyse durchgeführt. Die Strategie führt zu effektiven und angemessenen Sicherheitsmaßnahmen, birgt aber einen großen Aufwand von Wochen bis Monaten und somit auch hohe Kosten. Dabei ist die Gefahr gegeben, dass ein kritisches Risiko nicht rasch genug erkannt wird und Schutzmaßnahmen damit nicht rechtzeitig getätigt werden.

Die detaillierte Risikoanalyse umfasst folgende acht Schritte [Sihb04, S. 30-31]:

„Schritt 1: Abgrenzung des Analysebereiches
Hier ist das zu analysierende IT-System zu spezifizieren und anzugeben, ob und in welchem Maße auch andere Objekte (z.B. Gebäude und Infrastruktur) in die Analyse einbezogen werden sollen.

***Schritt 2: Identifikation der bedrohten Objekte** ("Assets")*
Ziel dieses Schrittes ist die Erfassung aller bedrohten Objekte, die innerhalb des im vorangegangenen Schritt festgesetzten Analysebereiches liegen.

Schritt 3: Wertanalyse
In diesem Schritt wird der Wert der bedrohten Objekte ermittelt. Die Wertanalyse umfasst im Einzelnen:

- *die Festlegung der Bewertungsbasis für Sachwerte*
- *die Festlegung der Bewertungsbasis für immaterielle Werte*
- *die Ermittlung der Abhängigkeiten zwischen den Objekten*
- *die Bewertung der bedrohten Objekte*

Schritt 4: Bedrohungsanalyse
Die Objekte sind vielfachen Bedrohungen ausgesetzt, die sowohl aus Nachlässigkeit und Versehen als auch aus Absicht resultieren können. Die Bedrohungsanalyse umfasst:

- *die Identifikation möglicher Bedrohungen (Katastrophen, Fehlbedienung, bewusste Angriffe) und möglicher Angreifer (Mitarbeiter, Leasingpersonal, Außenstehende,...)*
- *die Ermittlung der Eintrittswahrscheinlichkeiten*

Schritt 5: Schwachstellenanalyse

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Zu untersuchen sind dabei insbesondere die Bereiche Organisation, Hard- und Software, Personal sowie Infrastruktur.

Schritt 6: Identifikation bestehender Sicherheitsmaßnahmen

Zur Vermeidung unnötiger Aufwendungen und Kosten sind die bereits existierenden Sicherheitsmaßnahmen zu erfassen und auf ihre Auswirkungen hinsichtlich der Gesamtsystemsicherheit sowie auf korrekte Funktion zu prüfen.

Geplante neue Sicherheitsmaßnahmen müssen mit den existierenden kompatibel sein und eine wirtschaftlich und technisch sinnvolle Ergänzung darstellen.

Schritt 7: Risikobewertung

In diesem Schritt werden die Einzelrisiken und das Gesamtrisiko ermittelt und bewertet.

Schritt 8: Auswertung

Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse ab.“

Bei der Durchführung einer Risikoanalyse sind folgende Prinzipien zu beachten:

- Das gesamte Verfahren muss transparent gemacht werden.
- Es dürfen keine versteckten Annahmen getroffen werden, die z.B. dazu führen, dass Bedrohungen unbetrachtet bleiben.
- Alle Bewertungen müssen begründet werden, um subjektive Einflüsse zu erkennen und so weit wie möglich zu vermeiden.
- Alle Schritte müssen so dokumentiert werden, dass sie später auch für andere nachvollziehbar sind. Ein derartiges Vorgehen erleichtert auch eine spätere Überarbeitung des IT-Sicherheitskonzeptes.
- Der Aufwand für die Durchführung des Verfahrens sollte dem Wert der IT Anwendungen und den Werten der Institution im Allgemeinen angemessen sein.

.

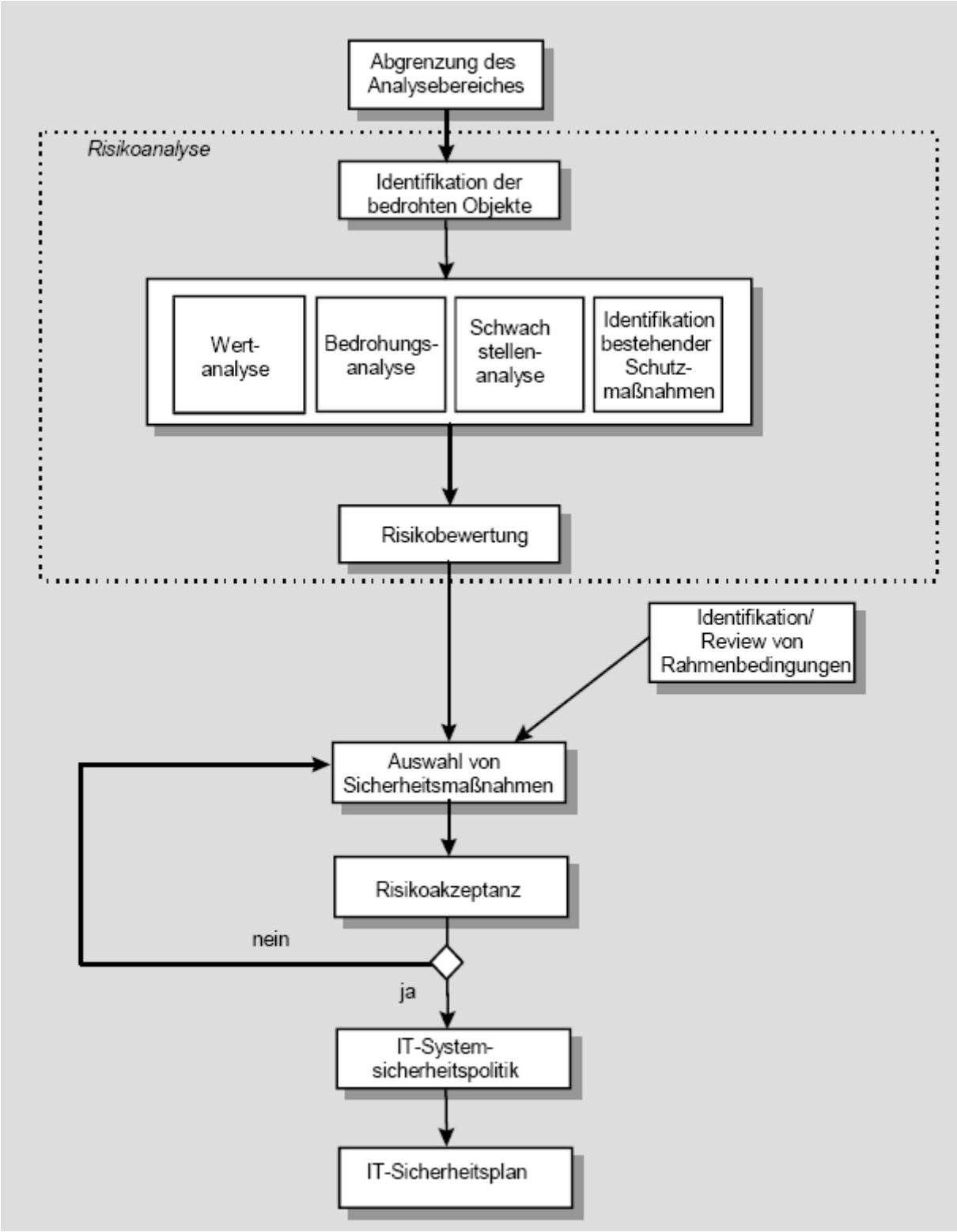


Abbildung 19: Risikomanagement mit detaillierter Risikoanalyse [Sihb04]

3.7.3 Risikoanalyse nach Grundschutzansatz

Ziel beim Grundschutzansatz aus dem deutschen Grundschutzhandbuch ist es, den Aufwand für die Erstellung eines IT-Sicherheitskonzeptes angemessen zu begrenzen. Dabei wird von einer pauschalierten Gefährdungslage ausgegangen und auf eine detaillierte Analyse verzichtet. Die Auswahl der Sicherheitsmaßnahmen erfolgt auf Basis vorgegebener Kataloge. Dadurch wird der Aufwand stark reduziert und der Einsatz von Grundschutzmaßnahmen führt rasch zu einem hohen Sicherheitsniveau. Dem gegenüber steht der Nachteil, dass falsch gewählte Kategorien Kosten verursachen oder Risiken bestehen lassen können.

Der Grundschutzansatz wird besonders unter folgenden Umständen empfohlen [Sihb04, S. 40]:

- *„Wenn feststeht, dass im betrachteten Bereich nur IT-Systeme mit niedrigem oder mittlerem Schutzbedarf zum Einsatz kommen.*
- *Falls in einem Bereich (IT-System, Abteilung,...) noch keine oder offensichtlich zu schwache Sicherheitsmaßnahmen vorhanden sind, kann die Realisierung von Grundschutzmaßnahmen dazu beitragen, rasch ein relativ gutes Niveau an IT Sicherheit zu erreichen. In diesem Fall sollte aber in einem nachfolgenden Schritt geprüft werden, ob das erreichte Niveau bereits ausreichend ist oder weitere Analysen und Maßnahmen erforderlich sind.*
- *Als Teil eines umfassenden Risikoanalysekonzeptes ("kombinierter Ansatz"): Wird zunächst in einem ersten Schritt festgestellt, welche IT-Systeme besonders schutzbedürftig sind ("Schutzbedarfsfeststellung"), so besteht die Möglichkeit, den Arbeitsaufwand für die Risikoanalyse und die Auswahl spezifischer Sicherheitsmaßnahmen auf diese hochschutzbedürftigen Systeme zu konzentrieren. Für alle anderen Systeme können Grundschutzmaßnahmen eingesetzt werden, ohne damit unangemessene Sicherheitsrisiken einzugehen.“*

Der Risikoanalyse-Grundschutzansatz besteht dabei aus folgenden Schritten [Sihb04, S 41]:

***„Schritt 1: Nachbildung eines IT-Systems** oder eines IT-Verbundes (Kombination mehrerer IT-Systeme) durch vorhandene Bausteine ("Modellierung")*

***Schritt 2: Soll-Ist-Vergleich** zwischen vorhandenen und empfohlenen Maßnahmen.“*

Bei der Modellierung gibt das Grundschutzhandbuch einen Bausteinkatalog [Gshb04, S. 42] vor der folgende Themen beinhaltet:

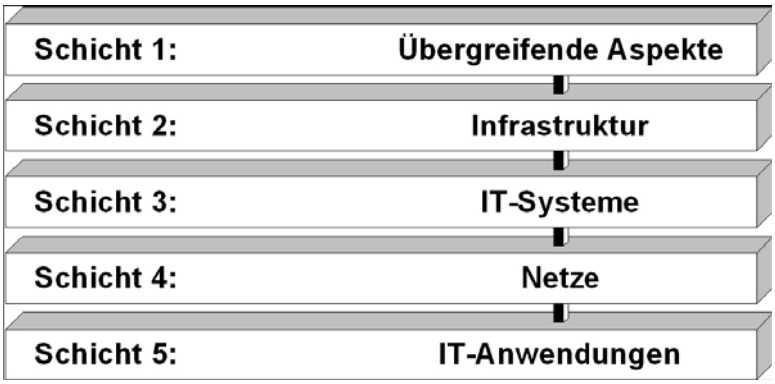


Abbildung 20: Schichten des IT-Grundschutzmodells [Bsi05/3]

*„**Schicht 1** umfasst die **übergreifenden IT-Sicherheitsaspekte**, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. (unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Virenschutzkonzept)*

***Schicht 2** befasst sich mit den **baulich-technischen Gegebenheiten**, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. (Gebäude, Serverraum, Schutzschrank, häuslicher Arbeitsplatz)*

***Schicht 3** betrifft die einzelnen **IT-Systeme** des IT-Verbunds. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. (TK-Anlage, Laptop, Clients)*

***Schicht 4** betrachtet die **Vernetzungsaspekte** der IT-Systeme, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. (Heterogene Netze, Modems, Remote Access)*

***Schicht 5** schließlich beschäftigt sich mit den eigentlichen **IT-Anwendungen**, die im IT-Verbund genutzt werden. (E-Mail, Webserver, Faxserver, Datenbanken)“*

3.7.4 Kombinierter Risikoanalyseansatz

Der kombinierte Ansatz vereint beide bisher beschriebenen Strategien und ihre Vorteile. Durch die Grundschutzanalyse wird Zeit und Kosten gespart, durch die detaillierte Risikoanalyse werden hohe Sicherheitsrisiken reduziert.

Dabei wird zuerst eine Schutzbedarfsfeststellung durchgeführt bei der die IT-Systeme in eine von drei Kategorien eingeteilt werden. Das österreichische IT-Sicherheitshandbuch fasst dabei die Kategorien „*hoch*“ und „*sehr hoch*“ zusammen, behandelt somit nur zwei Kategorien im Gegensatz zum deutschen Grundschutzhandbuch.

Schutzbedarfskategorien	
nieder bis mittel	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 3: Schutzbedarfskategorien nach [BSI05]

IT-Systeme der Schutzbedarfskategorie "*nieder bis mittel*" werden einer Grundschutzanalyse unterzogen, während IT-Systeme der Schutzbedarfskategorie "*hoch*“ und „*sehr hoch*" einer detaillierten Risikoanalyse zu unterziehen sind. Dabei sind laut IT-Sicherheitshandbuch zwei Varianten möglich [Sihb04, S. 44]:

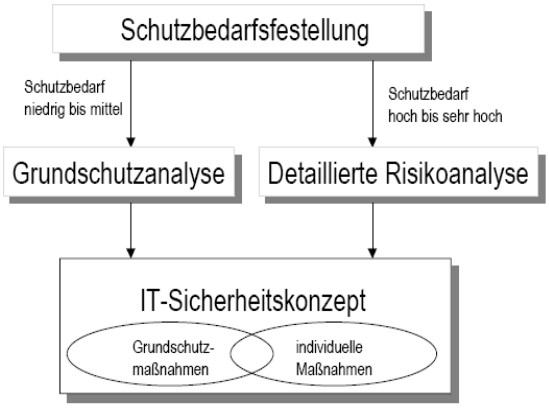


Abbildung 21: kombinierter Ansatz Variante 1

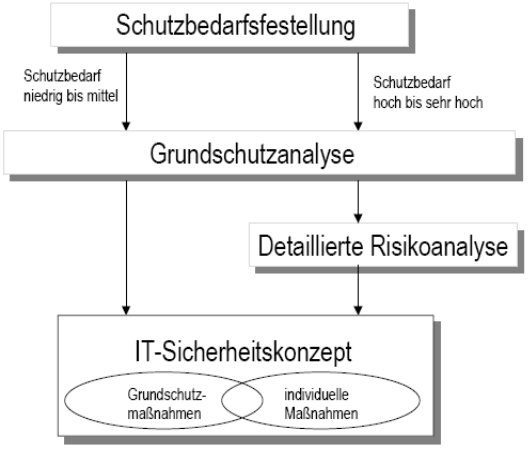


Abbildung 22: kombinierter Ansatz Variante 2

Bei Variante 1 wird ein IT-System nur einer Risikoanalyse unterzogen, je nach dem festgestellten Schutzbedarf. Dabei können bei der detaillierten Risikoanalyse durch den größeren Zeitaufwand wichtige Sofortmaßnahmen womöglich erst zu spät erkannt und

umgesetzt werden. Bei Variante 2 werden zuerst alle IT-Systeme einer Grundschutzanalyse unterzogen, bei jenen mit dem Schutzbedarf „hoch“ und „sehr hoch“ wird zusätzlich eine detaillierten Risikoanalyse durchgeführt.

Meist ist der kombinierte Ansatz am sinnvollsten, da rasch ein guter Sicherheitslevel erreicht wird und der Grossteil des Aufwandes für hochsicherheitsbedürftige Systeme verwendet werden kann. Es besteht lediglich das Risiko dass ein IT-System in die falsche Kategorie mit niedrigem Schutzbedarf zugeteilt wird und somit für dieses System keine detaillierte Risikoanalyse erfolgt.

4 Normen und Standards

4.1 ISO 17799

Die ISO/IEC17799:2000 ist ein internationaler Standard, welcher verschiedene Kontrollmechanismen für die Informationssicherheit beschreibt. Die ISO 17799 (Code of practice for information security management) entspricht inhaltlich dem British Standard 7799-1:1999.
Es werden dabei Erfahrungen, Verfahren und Methoden nach dem „Best practice“ Ansatz dargestellt. Die ISO 17799 ist nicht frei verfügbar, er muss erworben werden. Ein wesentlicher Teil bei diesem Standard ist das Risikomanagement. Der Standard ist hauptsächlich für die Sicherheitsbeauftragten von Behörden und große Unternehmen sinvoll, für Privatpersonen und KMUs ist er nicht geeignet.

Ziel der ISO 17799 ist es, eine umfassende Sammlung von Maßnahmen bereitzustellen. Dabei unterteilt der Standard sich in zwei Teile: Teil 1 gibt die einzelnen Maßnahmen an und Teil 2 ist die Basis für ein Informationssicherheits-Managementsystems. Dieser Aufbau zeigt, dass die ISO 17799 die Grundlage für das deutsche Grundschutzhandbuch ist.

Die ISO 17799 unterteilt sich in zehn Hauptkapitel:

- Informationssicherheitspolitik
- Computer- und Netzwerkmanagement
- Sicherheitsorganisation
- Zugangskontrolle
- Klassifizierung und Wert-Überwachung
- Systementwicklung und Wartung
- Sicherheit beim Personal
- Geschäftskontinuitätsplanung
- Physische und umgebungsbezogene Sicherheit
- Erfüllung der Verpflichtungen

Die Norm beschäftigt sich hauptsächlich mit dem Management von Informationssicherheit, dabei wird folgende Vorgehensweise verwendet:

Definition der Sicherheitspolitik, Bestimmung des Anwendungsbereichs des Managementssystems für Informationssicherheit, Durchführung einer angemessenen Risikoanalyse, Identifizierung der Risikobereiche, Auswahl der Sicherheitsziele und -maßnahmen, sowie Erklärung zur Anwendbarkeit der Maßnahmen.

Die Norm enthält sehr generische Sicherheitsmaßnahmen, und geht nicht auf genauere technische Details und Produkte ein. Dabei wird ein mittleres Sicherheitsniveau angestrebt, weshalb die Norm für hohe Sicherheitsansprüche nicht geeignet ist. Der Aufwand für die Umsetzung hängt von der Wahl der Risikoanalyse ab. Generell ist der Aufwand eher mittel bis hoch einzustufen.

4.2 IT-Grundschutzhandbuch des BSI

Im IT-Grundschutzhandbuch werden Standard-Sicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und IT-Anwendungen dienen kann.

Dabei definiert das Grundschutzhandbuch eine große Anzahl von **Bausteinen**, **Gefährdungskatalogen** und **Maßnahmenkatalogen**:

Bausteine: Die Bausteine der IT-Grundschutz Kataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen und IT-Systeme sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen. Die Bausteine sind in die folgenden Kataloge gruppiert [BSI05]:

- *B 1: Übergeordnete Aspekte der IT-Sicherheit* (Organisation, Personal, Outsourcing,..)
- *B 2: Sicherheit der Infrastruktur* (Verkabelung, Serverraum, Schutzschränke,..)
- *B 3: Sicherheit der IT-Systeme* (Unix, Windows Clients, Windows Server, TK-Anlage,..)

- *B 4: Sicherheit im Netz* (Netzmanagement, LAN-Anbindung, Remote Access,..)
- *B 5: Sicherheit in Anwendungen* (E-Mail, Webserver, Datenbanken,..)

Gefährdungskataloge: Dieser Bereich enthält die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. Die Gefährdungen sind in fünf Kataloge gruppiert [BSI05]:

- *G 1: Höhere Gewalt* (Personalausfall, Kabelbrand, Naturkatastrophen, ..)
- *G 2: Organisatorische Mängel* (fehlende Regelungen, unzureichende Wartung, Verstöße gegen das Urheberrecht,..)
- *G 3: Menschliche Fehlhandlungen* (fehlerhafte Administration, ungewollte Datenfreigaben, fahrlässiges Löschen,..)
- *G 4: Technisches Versagen* (Datenbankausfall, Ausfall der Stromversorgung, defekte Datenträger,..)
- *G 5: Vorsätzliche Handlungen* (unberechtigte IT-Nutzung, Viren, Spyware, Mitlesen von E-Mails,..)

Maßnahmenkataloge: Dieser Teil beschreibt die in den Bausteinen der IT-Grundschutz-Kataloge zitierten IT-Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Maßnahmenkataloge gruppiert [BSI05]:

- *M 1: Infrastruktur* (Feuerlöscher, Einbruchschutz, Klimatisierung,..)
- *M 2: Organisation* (Datenträgerverwaltung, Verantwortlichkeiten festlegen, Vergabe von Berechtigungen,..)
- *M 3: Personal* (Schulungen, Vertretungsregelungen, Sensibilisierung der Mitarbeiter,..)
- *M 4: Hard- und Software* (Passwortschutz, Bildschirmsperre, Test neuer Hardware,..)
- *M 5: Kommunikation* (Übersicht über Netzdienste, Verwenden von Verschlüsselung, Sichere Mail-Client Einstellungen,..)
- *M 6: Notfallvorsorge* (Notfall-Handbuch erstellen, Abschließen von Versicherungen, Lieferantenvereinarungen,..)

Das IT-Grundschutzhandbuch 2004 umfasst somit 58 Bausteine, 720 Maßnahmen auf 2900 Seiten. Es ist als Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten, und durch

seinen ganzheitlichen Ansatz eher als Nachschlagewerk und Referenz für IT-Sicherheit einzustufen.

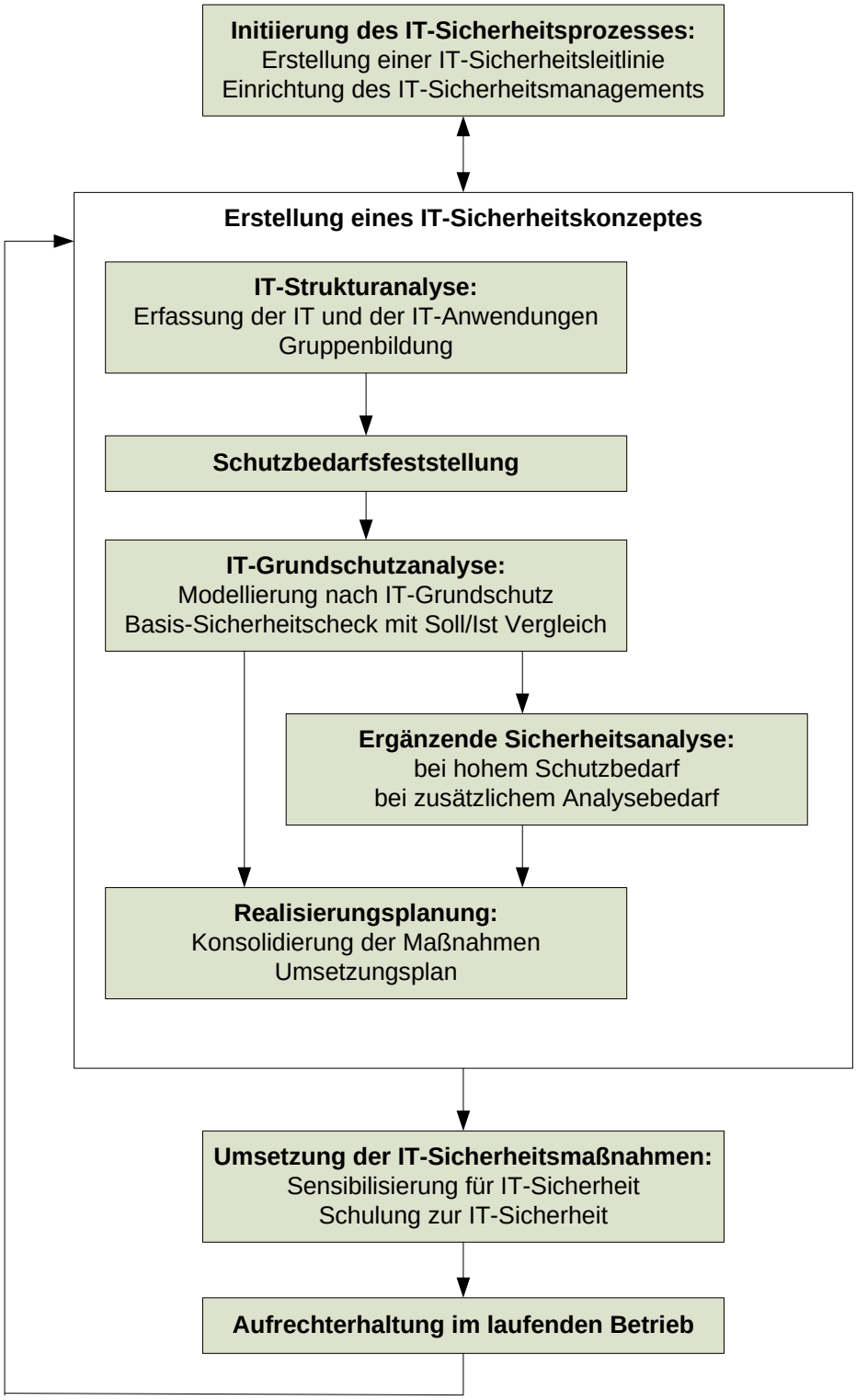


Abbildung 23: IT-Sicherheitsprozess nach BSI [BSI05]

Abbildung 25 zeigt den ganzheitlichen IT-Sicherheitsprozess wie er im Grundschutzhandbuch umgesetzt ist. Der Prozess beginnt mit der Definition der IT-Sicherheitsziele und der Einrichtung eines IT-Sicherheitsmanagements, dessen Aufgabe es ist, ein IT-Sicherheitskonzept zu erstellen und zu realisieren. Mit der Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb kehrt der IT-Sicherheitsprozess zur Erstellung des Sicherheitskonzepts zurück, um damit einen kontinuierlichen Prozess zu ermöglichen.

4.3 IT-Sicherheitshandbuch

Das österreichische IT-Sicherheitshandbuch ist sehr verwandt mit dem deutschen Grundschutzhandbuch. Es nimmt besondere Rücksicht auf Österreichische Gesetze und Normen. Ziel ist das Ermitteln von Sicherheitszielen und Strategien mit einer einheitlichen Vorgehensweise und Terminologie. An internationalen Standards fließt die ISO 13355, das IT-Grundschutzhandbuch und die ISO 17799 ein. Das Grundschutzhandbuch ist zusätzlich um Checklisten zur Überprüfung der Umsetzung erweitert.
Durch die etwas kleinere Ausführung als das Grundschutzhandbuch und zusätzlichen Checklisten ist das IT-Sicherheitshandbuch im Gegensatz zum Grundschutzhandbuch besser für KMUs geeignet.

Teil 1 umfasst den Sicherheitsmanagementprozess wie er in Abbildung 26 ersichtlich ist, und beinhaltet konkrete Anleitungen zur Etablierung eines umfassenden und kontinuierlichen IT-Sicherheitsprozesses.
Teil 2 beinhaltet IT-Sicherheitsmaßnahmen und deren Beschreibungen auf organisatorischer, personeller, infrastruktureller und technischer Ebene. Inhaltliches Ziel ist die Gewährleistung angemessener Standardsicherheitsmaßnahmen für IT-Systeme.

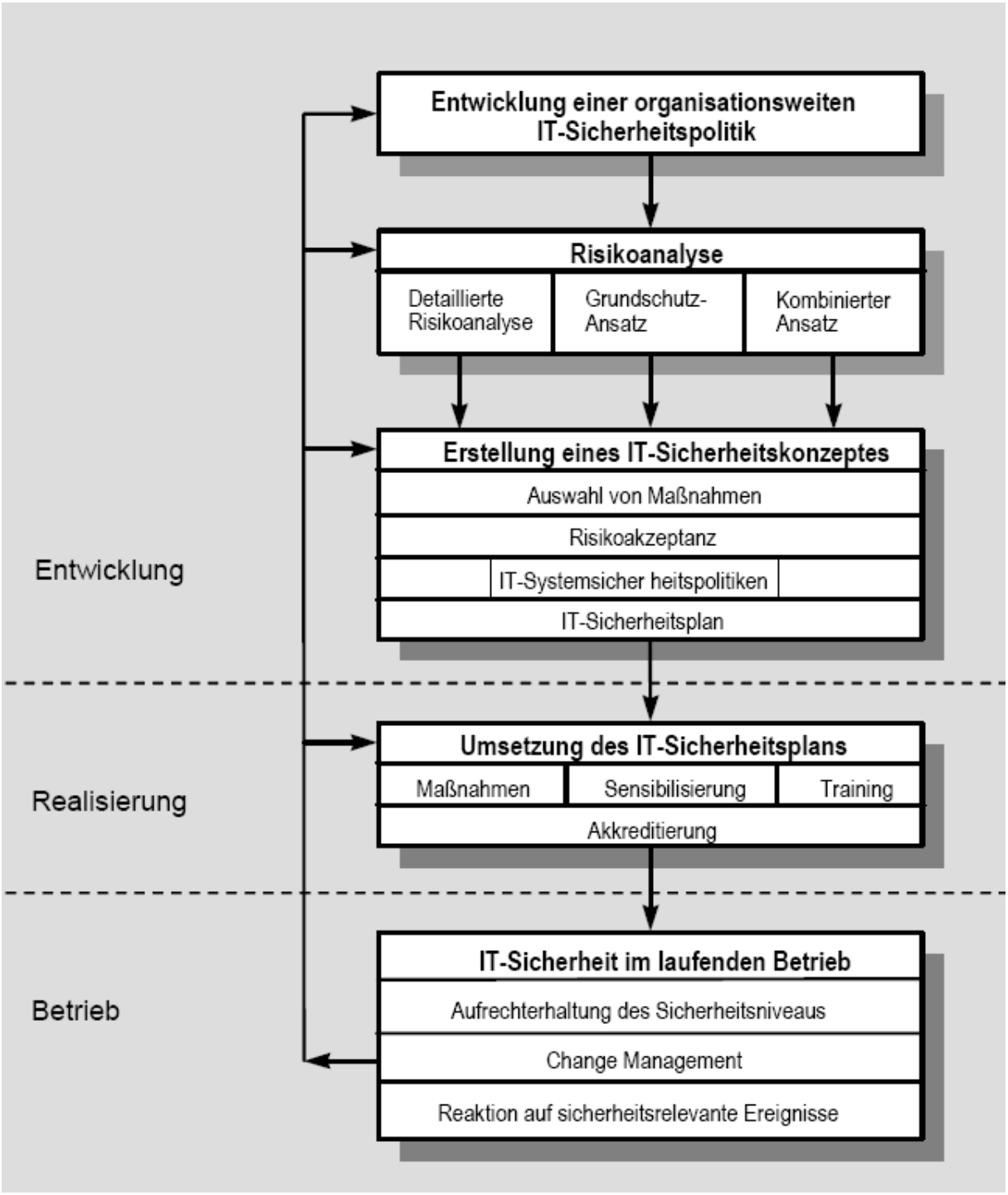


Abbildung 24: Aktivitäten im IT-Sicherheitsmanagement [Sihb04/2]

4.4 ITSEC / Common Criteris

Die ITSEC (Information Technology Security Evaluation Criteria) und Common Criteria definieren Prüfverfahren für sicherheitsrelevante Aspekte der IT, um diese nachvollziehbar und vergleichbar zu machen. Die ITSEC ist ein europäischer Standard, welcher 1991 veröffentlicht wurde. Die Common Criteria sind quasi der Nachfolger der ITSEC und erstmals 1999 erschienen. Sie sollen auf internationaler Ebene Datensicherheit und Datenschutz vergleichbar machen.

Diese Kriterien haben eine sehr technische Sicht und sind eher für Produkte und Systeme geeignet als zur Etablierung eines Sicherheitsprozesses. Dabei geben die Kriterien Prüfanweisungen mit funktionalen und qualitativen Aspekten vor. Somit sind sie für Hersteller von IT-Systemen, IT-Produkten und IT-Komponenten gut verwendbar.

Die Common Criteria umfassen drei Teile [BSI05, zusammengefasst]:

***Teil 1**: Einführung und allgemeines Modell:* Hier werden die Grundlagen der IT-Sicherheitsevaluation und der allgemeine Geltungsbereich der Comon Criteria erläutert. In den Anhängen werden Schutzprofile und Sicherheitsvorgaben für den zu prüfenden Evaluationsgegenstand beschrieben.

***Teil 2**: Funktionale Sicherheitsanforderungen:* Dieser Teil enthält einen umfangreichen Katalog von Funktionalitätsanforderungen. Er stellt ein empfohlenes Angebot für die Beschreibung der Funktionalität eines Produktes bzw. Systems dar, von dem jedoch in begründeten Fällen abgewichen werden kann. Im Anhang finden sich Hintergrundinformationen. Zusätzlich werden Zusammenhänge zwischen Bedrohungen, Sicherheitszielen und funktionalen Anforderungen aufgezeigt.

***Teil 3**: Anforderungen an die Vertrauenswürdigkeit:* Hier sind die Anforderungen an die Vertrauenswürdigkeit aufgelistet. Wichtig ist, dass ein Evaluationsergebnis immer auf einer Vertrauenswürdigkeitsstufe basieren sollte, eventuell ergänzt durch weitere Anforderungen. Die Common Criteria geben sieben hierarchische Vertrauenswürdigkeitsstufen vor.

4.5 Vergleich der Kriterien

Ein Vergleich kann unter anderem nach folgenden Gesichtspunkten erfolgen [Init01]:

- *Bezieht sich der Inhalt des jeweiligen Kriterienwerks eher auf einzelne Produkte oder Komponenten innerhalb einer IT-Landschaft oder beschäftigt sich das Kriterienwerk eher mit dem Zusammenspiel mehrerer Komponenten in einem Gesamtsystem?*

- *Sind die in dem jeweiligen Kriterienwerk behandelten Teilaspekte eher technischer oder nichttechnischer (z. B. organisatorischer) Art?*

Die beschriebenen Kriterien lassen sich somit wie folgt in ein Diagramm einteilen:

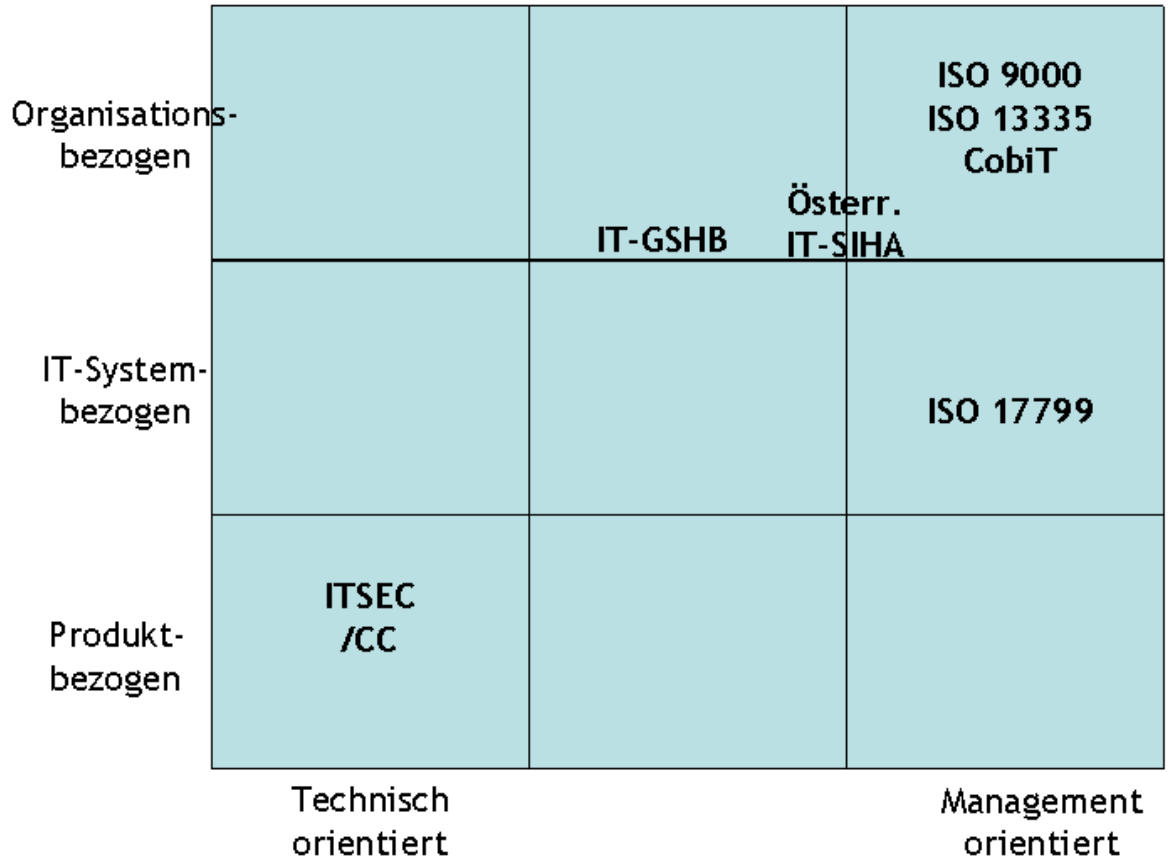


Abbildung 25: Einteilung von Sicherheitskriterien [Init01]

Es zeigt sich, dass kein IT-Sicherheitskriterienwerk in der Praxis alle Ebenen abdecken kann, weshalb die Auswahl des richtigen Kriterienwerkes grundlegend davon abhängt, ob eher eine Produktbezogene oder Organisationsbezogene Sicherheitsanforderung besteht. Durch

Kombination verschiedener Kriterienwerke können natürlich Produkt- und Systembezogene Kriterien untersucht werden, was jedoch in einem höheren Zeit- und Kostenaufwand resultiert.

5 Policies

Zum leichteren Verständnis wie eine IT Security Policy aufgebaut werden kann, folgen einige Beispiele aus verschiedenen Quellen zu unterschiedlichen Themenbereichen. Da Policies immer individuell für das jeweilige Unternehmen oder Institution entwickelt werden müssen, sollen diese Policies nicht als Vorlage sondern nur als Input dienen. Eine Policy muss immer auf das Unternehmen und das geforderte Sicherheitsniveau angepasst sein, um die richtigen Regelungen zu treffen.

5.1 Virtual Private Networks Policy

Aus Praxisbeispielen des Bundesamts für Sicherheit in der Informationstechnik [BsiPol05]:

Übersicht

Zielgruppe (Wer muss befolgen)	*IT-Führungskräfte und Netzwerkadministratoren*
Zusammenfassung (Was:)	*Auswahl, Aufbau und Betrieb von Virtual Private Networks*
Zweck (Warum:)	*Systemspezifische Regelungen in Bezug auf VPN*
Übergeordnete Regeln	• *IT-Infrastruktur – Allgemeine Regelungen* • *Netzwerke – Allgemeine Regelungen*

Einführung

Ein Virtual Private Network (VPN) ist ein virtuelles Netz zur Übermittlung von privaten Daten. Der Begriffe „virtuell“ und „privat“ bedeuten dabei, dass die darunter liegende Netzinfrastruktur zwischen mehreren (virtuellen) Netzen geteilt wird, die Netzverbindung aber aus Sicht des Benutzers wie ein privates Netz wirkt. Unter Verwendung dieser Definition können auch ATM, Frame Relay und MPLS als VPNs bezeichnet werden. Die häufigste Variante ist aber der Einsatz von VPNs über das Internet als zugrunde liegende Netzinfrastruktur.

Der Basisschutz von VPN´s beinhaltet nicht die Verschlüsselung des Datenverkehrs. Er basiert auf der logischen Trennung der VPNs und auf dem Vertrauen, dass der Betreiber der Infrastruktur eine Manipulation des Netzes und der darauf transportierten Daten selber nicht vornimmt bzw. eine Manipulation durch Dritte verhindert.

Wird dies nicht als ausreichend erachtet, müssen die Daten, die über das VPN laufen, verschlüsselt werden. Die gängige Methode dies zu tun, ist die Verwendung des offenen Standards IPSec, eines Layer-3-Tunneling Verfahrens. IPSec lässt sich z. B. über ein MPLS Netzwerk legen, um auch hier die Integrität der übertragenen Daten zu gewährleisten.

Regelungen

Es gelten die allgemeinen Regelungen zum Netzwerk. Darüber hinaus gelten folgende weitere Regelungen.

R 1:	*Bei VPN-Kopplung von Netzen über Netzwerk-Infrastrukturen, die nicht als ausreichend sicher erachtet werden, wird eine Verschlüsselungstechnologie eingesetzt.*
R 2:	*Gängige Firewall-Produkte können in der Regel auch als VPN Konzentratoren oder Endpunkte eingesetzt werden. Bei VPN-Verbindungen für Anwendungen, bei denen die Verbindung geschäfts- oder sicherheitskritisch ist, werden die VPN Systeme von anderen Systemen getrennt betrieben.*

So werden die Risiken, die bei einer Firewall als Tor zu einem „unsicheren" Netzwerk bestehen, nicht auf das VPN übertragen.

R 3:	*Ein VPN-Client-Zugang von einem Drittnetz muss vor der Durchleitung in das interne Netz durch die Firewall authentifiziert werden.*

R 4:	*Internet-basierende VPN-Lösungen werden nicht für geschäfts- oder sicherheitskritische Kommunikationsverbindungen eingesetzt, bzw. nur dann, falls eine Ausweichlösung über ein anderes Kommunikationsmedium existiert.*

Die Verfügbarkeit des öffentlichen Internets kann nicht in ausreichendem Maße garantiert werden.

Überprüfung und Durchsetzung

Die Überwachung und Durchsetzung der oben genannten Regeln, sollte nach Möglichkeit einheitlich gestaltet sein. Es sind daher die übergeordneten Regelbereiche zu berücksichtigen.

Zusätzlich gilt:

R 5:	*Die VPN Schnittstellen werden in regelmäßigen Abständen durch einen Penetrationstest geprüft.*

5.2 Interne Web Services (Intranet) Policy

Aus Praxisbeispielen des Bundesamts für Sicherheit in der Informationstechnik [BsiPol05]:

Übersicht

Zielgruppe *(Wer muss befolgen)*	*IT-Führungskräfte und Netzwerkadministratoren*

Zusammenfassung (Was:)	*Aufbau, Betrieb und zur Überprüfung eines Dienstes, der Informationen unternehmensweit und webbasiert zur Verfügung stellt (Intranet)*
Zweck (Warum:)	*Schutz des Austausches von internen Informationen im Intranet, Verhaltensmaßnahmen in Bezug auf den Zugriff auf Informationen des Intranets*
Übergeordnete Regeln	*Zentrale Systeme – Allgemeine Regelungen*

Einführung

Der Aufbau interner Web-Services erfreut sich zunehmender Beliebtheit. Arbeitsrelevante Informationen könne über dieser Medium zentral allen Mitarbeitern zur Verfügung gestellt werden. Wegen der wachsenden Bedeutung des Intranets für die Arbeitsabläufe in Unternehmen sollten auch geeignete Schutzmaßnahmen getroffen werden.

Regelungen

R 6:	*Alle Websites enthalten Erklärungen zum Datenschutz und zum Schutz der Privatsphäre.*
R 7:	*Es existiert ein technischer Betriebsstandard für interne Web-Server.*

Es gibt Regeln, die für den aktuellen Zeitraum oder das genau Einsatzgebiet sinnvoll sind. Diese eher Technischen Regeln sollten an den jeweiligen Bedarf angepasst und periodisch überprüft werden, um sicherzustellen, dass sie im zeitlichen und funktionalen Kontext nach wie vor angemessen sind. Ein Beispiel dafür, ist der unten verbotene Zugriff per FTP (File Transfer Protocol).

Thema	***Standard***
Default Website Access	*Read only for all authenticated users*
Restricted Website Access	*Using IIS Access controls and underlying NT File/Dir ACLs.*
Anonymous Access	*Discouraged, however may be required for some websites*
Virtual Webs	*Allowed using http host headers*
Metabase back-ups	*Backups are taken every month (present)* *Twice per week (future)*
File Listing	***Prohibited** – File listing should be disabled*
Default Filename(s)	*Default.htm, default.asp*
Mail Enabled Websites (e.g. form mail	*CDONTS (See email codes of practice for guidance on relaying mail)*
FTP Service	***Disabled***
NNTP Service	***Disabled***
Registration for Global Search	*Site shall be registered in order to be indexed by Global Search*

Überprüfung und Durchsetzung

Die Überwachung und Durchsetzung der oben genannten Regeln sollte nach Möglichkeit einheitlich gestaltet sein. Es sind daher die übergeordneten Regelbereiche zu berücksichtigen.

5.3 Email Use Policy

Aus den Beispielpolicies des SANS Institute, Security Policy Project [SANS05]:

Email Use Policy

1.0 Purpose
To prevent tarnishing the public image of <COMPANY NAME> When email goes out from <COMPANY NAME> the general public will tend to view that message as an official policy statement from the <COMPANY NAME>.

2.0 Scope
This policy covers appropriate use of any email sent from a <COMPANY NAME> email address and applies to all employees, vendors, and agents operating on behalf of <COMPANY NAME>.

3.0 Policy
3.1 Prohibited Use. *The <COMPANY NAME> email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any <COMPANY NAME> employee should report the matter to their supervisor immediately.*

3.2 Personal Use.
Using a reasonable amount of <COMPANY NAME> resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a <COMPANY NAME> email account is prohibited. Virus or other malware warnings and mass mailings from <COMPANY NAME> shall be approved by <COMPANY NAME> VP Operations before sending. These restrictions also apply to the forwarding of mail received by a <COMPANY NAME> employee.

3.3 Monitoring
<COMPANY NAME> employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. <COMPANY NAME> may monitor messages without prior notice. <COMPANY NAME> is not obliged to monitor email messages.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	***Definition***
Email	*The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.*
Forwarded email	*Email resent from an internal network to an outside point.*
Chain email or letter	*Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.*
Sensitive information	*Information is considered sensitive if it can be damaging to <COMPANY NAME> or its customers' reputation or market standing.*
Virus warning.	*Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.*
Unauthorized Disclosure	*The intentional or unintentional revealing of restricted information to people, both inside and outside <COMPANY NAME>, who do not have a need to know that information.*

6 Tutorial zur Entwicklung von Security Policies

Das folgende Tutorial erklärt Schritt für Schritt, wie man bei der Entwicklung von Security Policies vorgehen soll. Dabei wird eine detaillierte Übersicht über den IT-Sicherheitsprozess gegeben. Die Präsentation richtet sich an Personen, welche sich noch nicht mit diesem Thema beschäftigt haben. Sie ist allgemein verfasst, damit die Inhalte für IT-Entscheider und Personen im Management sowie Mitarbeiter in nicht-technischen Positionen leicht verständlich sind. Besonderer Fokus liegt darin, Motivation zum Umsetzen einer Security Policy zu erzeugen und einseitige Sichtweisen wie „Sicherheit ist kompliziert und teuer“ abzubauen.

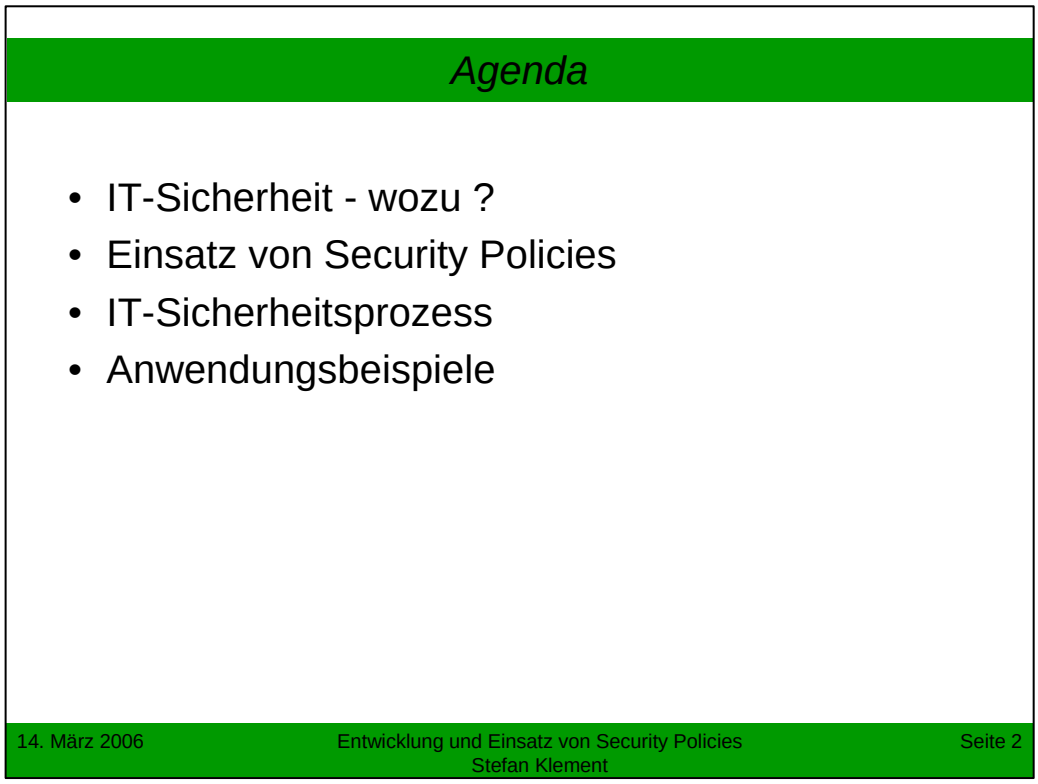
Für den Vortragenden sind unter den Folien Anmerkungen vorhanden und weitere Beispiele, sowie Links in die einzelnen Kapitel der Arbeit für eine weitere Vertiefung.

Johannes Kepler Universität Linz

Institut für Informationsverarbeitung und Mikroprozessortechnik

Entwicklung und Einsatz von Security Policies

Stefan Klement



Das folgende Tutorial erklärt Schritt für Schritt wie man bei der Entwicklung von Security Policies vorgehen soll. Dabei wird eine detaillierte Übersicht über den IT-Sicherheitsprozess gegeben. Dies soll für Personen ausgelegt sein, welche sich noch nicht mit diesem Thema beschäftigt haben. Das tutorial ist eher generell ausgeführt, so dass es für IT-Entscheider als auch Personen im Management und nicht technischen Positionen leicht verständlich ist. Besonderer Fokus liegt darin, Motivation zum Umsetzen einer Security Policy zu erzeugen.

Der Firmen Standort ist Linz, die Gründung erfolgte im Jahr 2000.

Ebit ist **IT-Spezialist** und **Softwareproduzent** im Bereich Kundenbeziehungsmanagement und IT-Outsourcing.

Die seit dem Jahr 2000 eigenentwickelte Lösung „Agilia“ ist eine webbasierte CRM Software. Sie ist als Gesammtlösung für Call und Customer Care sowie Contact Center optimal geeignet. Durch optionale Module ist „Agilia“ auch sehr einfach für den Vertriebs- und Help Desk Prozess einsetzbar.

Ebit setzt Projekte aus dem gesamten IT Bereich um. Darunter zählen Webshops, Firmenportale, IT-Infrastrukturprojekte als auch komplette Individual-programmierungen.

Für KMUs im Mittel- und Osteuropäischen Raum ist Ebit IT-Outsourcingpartner und betreut dabei die komplette IT-Infrastruktur (Netzwerk, Server, Arbeitsplätze, ..) als auch die Benutzer selbst. Im Rahmen der IT-Betreuung werden laufend Sicherheits- und Notfallkonzepte entwickelt und umgesetzt mit dem Ziel eine sichere, verfügbare und stabile IT-Umgebung zu schaffen.

Für den Vortragenden kann hier die Vorstellung des eigenen Umfeldes und Themengebietes erfologen.

IT-Sicherheit - wozu ?

<kes>/Microsoft-Sicherheitsstudie 2004
Bedeutung der verschiedenen Gefahrenbereiche

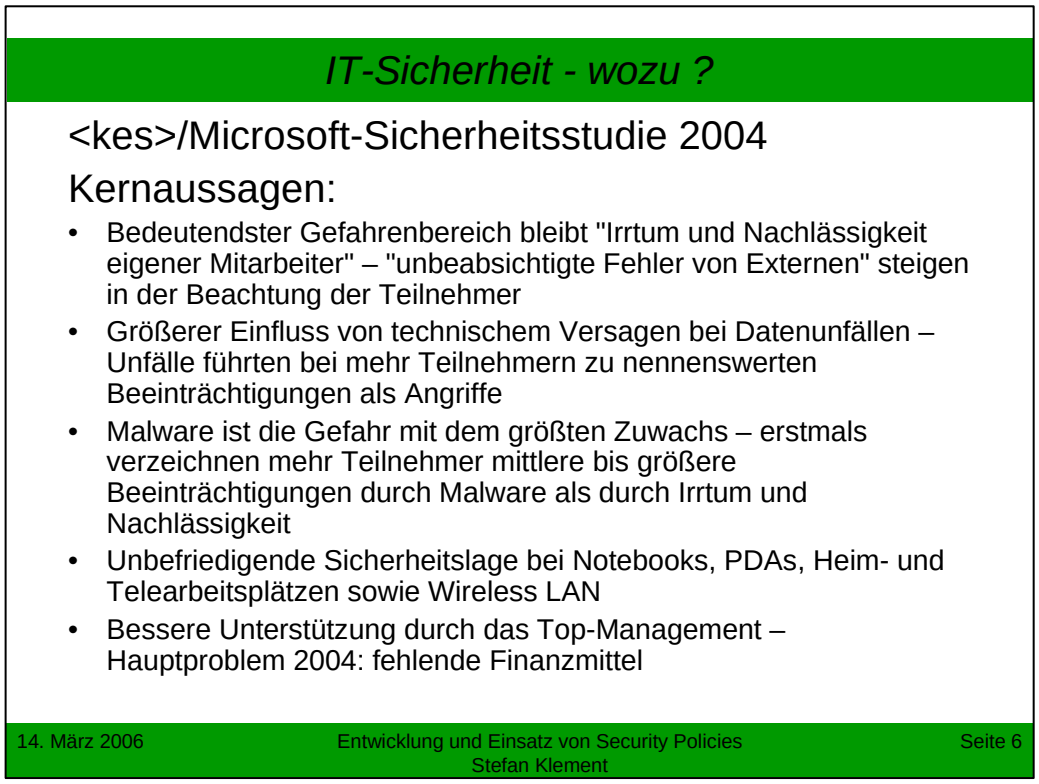
Gefahrenbereiche	Priorität	Schäden [%]
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	51
Malware (Viren, Würmer, Troj. Pferde,...)	2	54
Unbefugte Kenntnisnahme,Informationsdiebstahl,Wirtschaftsspionage	3	9
Software-Mängel/-Defekte	4	43
Hacking (Vandalismus, Probing, Missbrauch,...)	5	19
Hardware-Mängel/-Defekte	6	38
unbeabsichtigte Fehler von Externen	7	15
höhere Gewalt (Feuer, Wasser,...)	8	8
Manipulation zum Zweck der Bereicherung	9	8
Mängel der Dokumentation	10	17
Sabotage (inkl. DoS)	11	8
Sonstiges	12	3

14. März 2006 Entwicklung und Einsatz von Security Policies Seite 5
Stefan Klement

Die Studie des Onlinemagazines <kes> [Kes04] in Kooperation mit Microsoft basiert auf 163 eingegangenen Fragebögen.

Die Teilnehmer der <kes>-Sicherheitsstudien entstammen klassischerweise eher großen mittelständischen sowie Großunternehmen und -institutionen: Die durchschnittliche Mitarbeiterzahl beträgt über 4600, in der Summe repräsentieren die Befragten rund eine Dreiviertelmillion Beschäftigte in Deutschland.

Seit Beginn der <kes>-Studien nennen die Teilnehmer hier allem voran "Irrtum und Nachlässigkeit eigener Mitarbeiter" – so auch in diesem Jahr. Weiterhin folgen knapp dahinter als Gefahrenbereich mit der zweitgrößten Bedeutung Viren, Würmer und Trojanische Pferde (Malware), mit etwa demselben "Abstand" wie in der vorausgegangenen Studie von 2002.



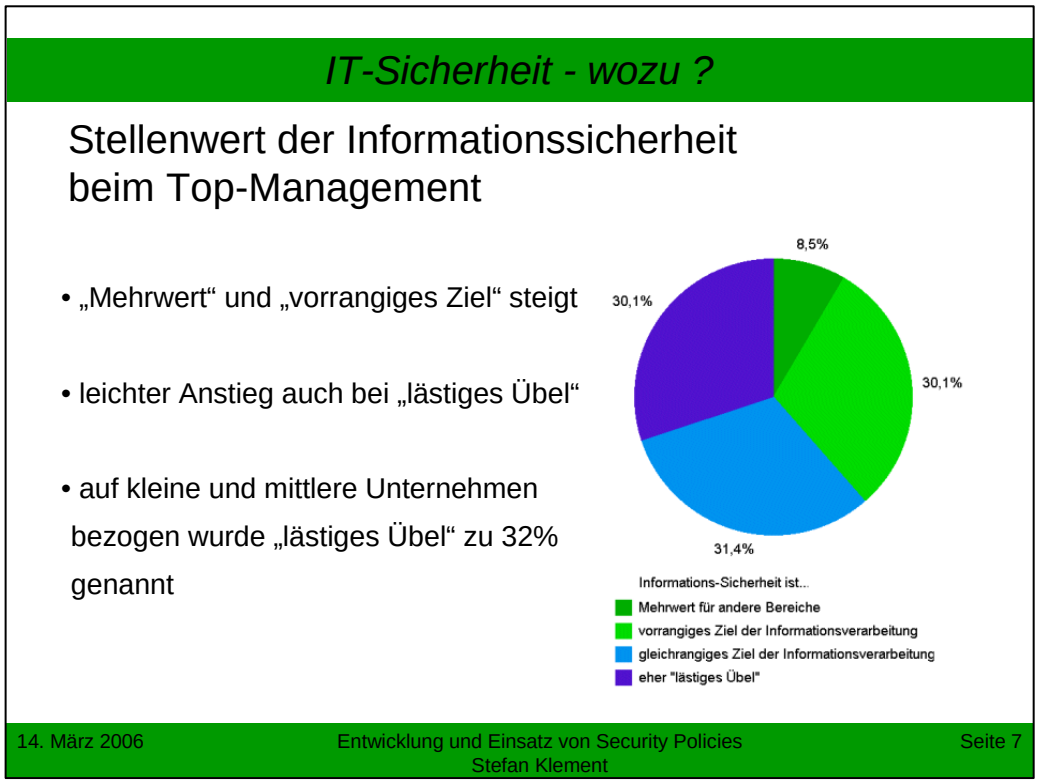
Schätzungen für die momentane Studie 2006:

•„unbeabsichtigte Fehler von Externen“ steigt in seiner Bedeutung.

(Ist man als Vortragender selbst „Extern“, sollte dieser Schätzung nicht zu viel Beachtung gewidmet werden.)

•„Hardware-Mängel/-Defekte“ Bedeutung sinkt leicht

•„Malware“ und „Hacking“ wird eine steigende Bedeutung prognostiziert



Aus <kes>-Sicherheitsstudie 2004 [Kes04]:

Stellenwert der Informations-Sicherheit beim Top-Management

Basis: 153 Antworten

Bei den Unternehmen mit mehr als 500 Mitarbeitern war zu erkennen:

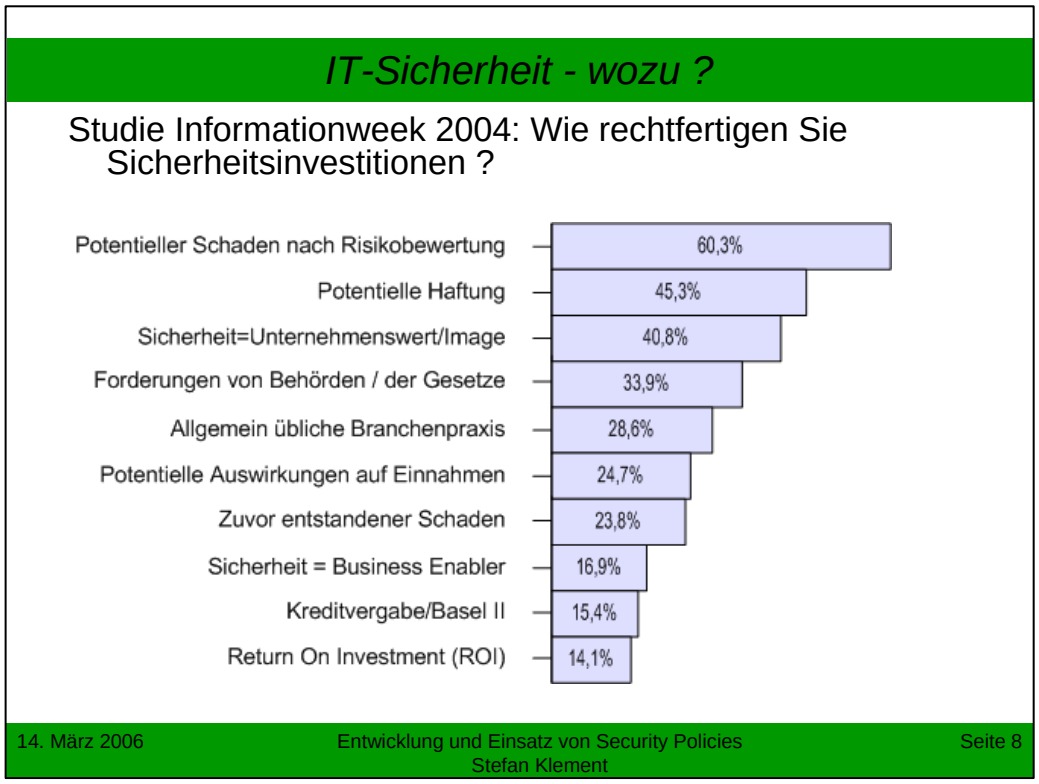
28 % Befürworter stehen hier 42 % "Gleichrangigkeits-Unterstützern", aber auch nur 29 % eher ablehnender Haltung gegenüber .

Das IT-Sicherheitsbewusstsein steigt mit der Unternehmensgröße und ist oft sehr von der Branche abhängig.

Gründe:

•Know-How

•Abhängigkeit von IT



In einer Studie der InformationWeek im Jahr 2004 [InfW04] wurde unter anderem gefragt wie IT Sicherheitsinvestitionen gerechtfertigt werden. Dabei wurden 842 Antworten von IT-Managern und Sicherheitsverantwortlichen zu über vierzig Fragen aus allen Bereichen der Informationssicherheit ausgewertet.

Den Schluss bildet der ROI, der bei Investitionen im Sicherheitsbereich keine oder nur eine sehr geringe Aussagekraft besitzt. Es liegt also nahe, als erstes mit einer groben Risikobewertung einen Sicherheitsprozess zu beginnen und sich ebenfalls über die Haftungsrisiken einen Überblick zu schaffen.

IT-Sicherheit - wozu ?

<kes>/Microsoft-Sicherheitsstudie 2004

Verbesserung der IT-Sicherheit wird behindert durch:

Hinderungsgrund	genannt von [%]
Es fehlt an Geld	62
Es fehlt an Bewusstsein bei den Mitarbeitern	51
Es fehlt an Bewusstsein und Unterstützung im Top-Management	45
Es fehlt an Bewusstsein beim mittleren Management	42
Es fehlen verfügbare und kompetente Mitarbeiter	33
Es fehlen die strategischen Grundlagen/ Gesamt-Konzepte	31
Die Kontrolle auf Einhaltung ist unzureichend	29
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	28
Es fehlen geeignete Methoden und Werkzeuge	18
Die vorhandenen Konzepte werden nicht umgesetzt	18
Es fehlen geeignete Produkte	17
Es fehlen realisierbare (Teil-)Konzepte	17

14. März 2006 Entwicklung und Einsatz von Security Policies Seite 9
Stefan Klement

Weitere Nennungen:

Anwendungen sind nicht für Informationssicherheits-Maßnahmen vorbereitet	17 %
Es fehlt an praxisorientierten Sicherheitsberatern	8 %
Sonstiges	6 %
keine Hindernisse	3 %

In den Studien der letzten Jahre war das fehlende Bewusstsein bei Mitarbeitern und Management am ausschlaggebensten. Im Jahr 2004 ist erstmals zu wenig Geld als Haupthindernis angegeben worden: Fast zwei Drittel (62 %) der Teilnehmer klagten über Behinderung durch finanzielle Beschränkung. (+16 %).

Positiv zeigte sich hingegen die Entwicklung der Awareness: Das mangelnde Bewusstsein bei den Mitarbeitern und Managern wurde von deutlich weniger Teilnehmern beklagt, belegt aber immer noch die Problem-Ränge zwei bis vier.

Details zur <KES> Studie:

Die Studie stellt auf fünfzehn Seiten detaillierte Fragen zur IT-Sicherheit und umfasst folgende Bereiche:

1. Aktuelle Risikosituation

2. ISi-Strategie und –Management

3. Informationsquellen und Schulung

4. Methoden und Maßnahmen

5. Bundesamt für Sicherheit in der Informationstechnik (BSI)

Als Beispiel werden hier einige ausgewählte Fragen angeführt [Kes04]:

1.02 Wie schätzen sie die Informationssicherheit in Ihrem Haus ein?
(sehr gut/gut/befriedigend/ausreichend/nicht ausreichend/ n.b) bezogen auf….
Rechenzentrum/Mainframe
Server
Clients/PCs
mobile Endgeräte
Teleworking-PCs
Speichermedien
IT-Netzwerk, kabelgebunden
IT-Netzwerk, drahtlos
TK-Netzwerk
Applikation/Geschäftsanwendungen

1.07 Häufigkeit und Aufwand von Sicherheitsvorfällen/Fehlalarm
(Häufigkeit des Auftretens x/Jahr / Ausfallzeit in Std. / Kosten) verursacht durch…
Virus/Wurm Infektion
Spyware-Befall
Malware-Fehlalarm (unbegründete Fehlermeldung)
unbegründete Warnung (Hoax)
(erfolgreicher) Online-Angriff
Phishing-Vorfall

2.01 Gibt es in ihrem Haus … ?

(ja/nein)

eine schriftlich fixierte Strategie für die Informationsverarbeitung

eine schriftlich fixierte Strategie für die Informationssicherheit

eine umfassendes, integriertes Sicherheitshandbuch

schriftlich fixierte spezifische ISi-Konzepte/Richtlinien

- zum Einsatz von Verschlüsselung
- zur Handhabung sensitiver/kritischer Daten
- zur Nutzung von Interner, E-Mail, …
- zum Softwareeinsatz auf PCs
- zur Nutzung mobiler Endgeräte (Notebook, PDA, ..)
- zur Nutzung mobiler Speicher und Plug&Play-Peripherie
- sonstige

schriftlich formulierte ISi-Maßnahme

4.11 Welche Log-Daten wertet ihr Haus aus?

(2x/Woche / seltener / anlassbezogen / keine Auswertung od. Protokollierung)

Anti-Virus-Lösungen

Firewalls

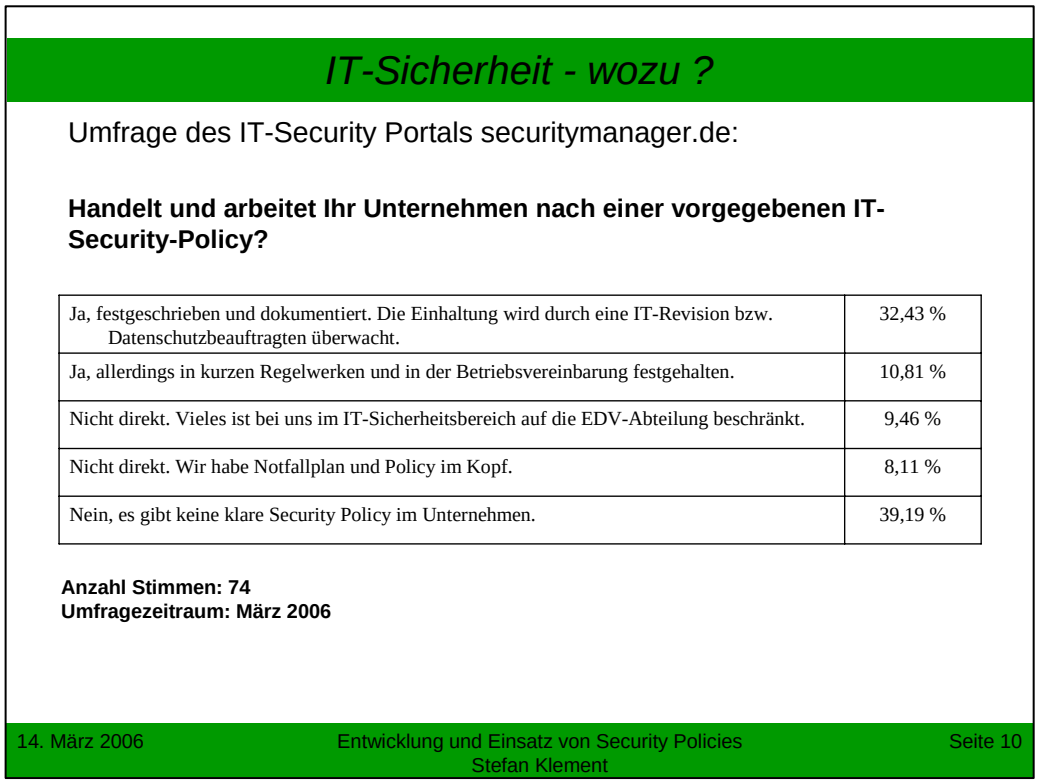
Intrusion Detection/Prevention Systems

Netzkomponenten (Router, Switches, ..)

Betriebssysteme

Web-/E-Commerce-Applikationen

sonstige Applikationen



Aktuelles Ergebnis ist abzufragen unter:

http://www.securitymanager.de/community/

Weitere Umfrage im Februar 2006:

Verwenden Sie Antiviren Software am Arbeitsplatz ?

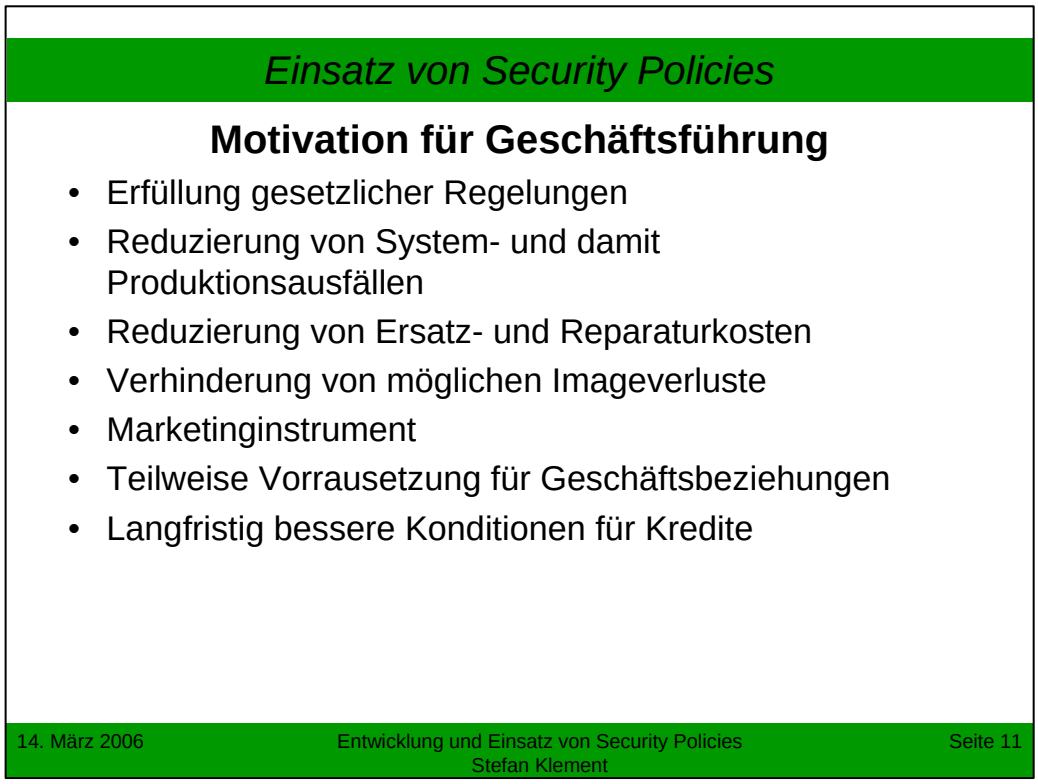
Ja: 89,74 %

Nein: 8,33 %

Geplant: 1,92 %

Anzahl Stimmen: 156

Aus der Umfrage lässt sich ableiten, dass ~50% der Unternehmen keine schriftlichen Aufzeichnungen besitzen!



- Erfüllung gesetzlicher Regelungen:
  Strafrecht, Haftung, Gesellschaftsrecht, Stand der Technik, Basel II

- Reduzierung von System- und damit Produktionsausfällen:
  monetärer Verlust durch Systemstillstand steigt mit Anzahl der Mitarbeiter

- Reduzierung von Ersatz- und Reparaturkosten

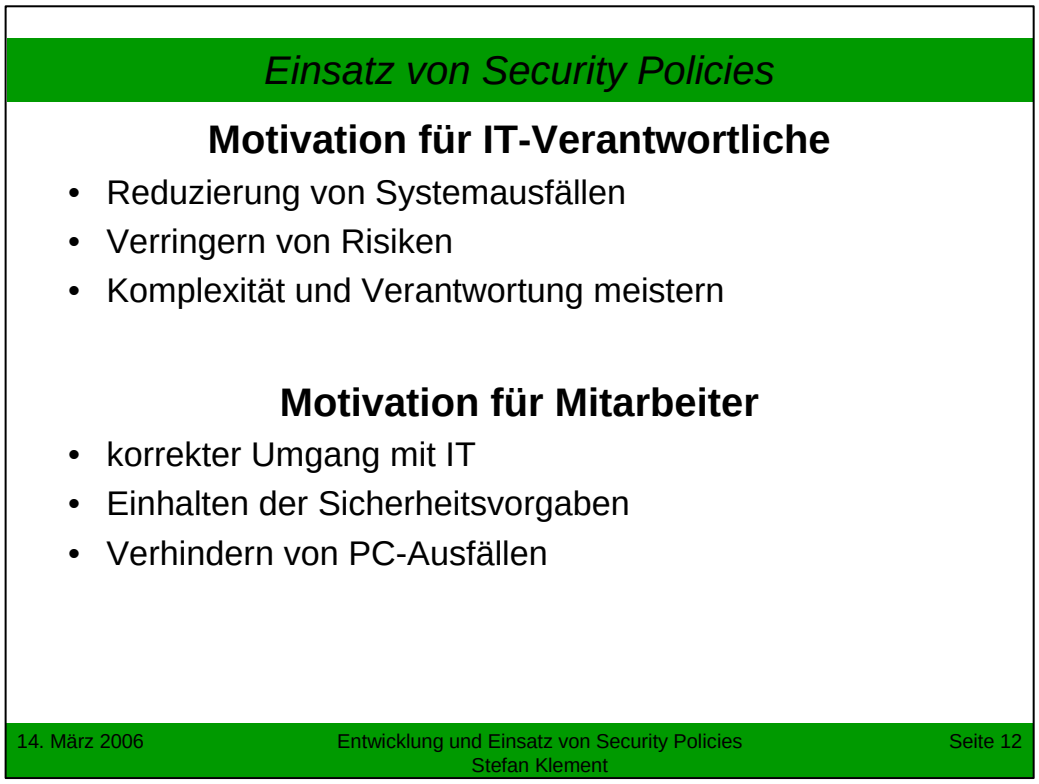
- Verhinderung von möglichen Imageverluste , z.B. bei Kreditkarteninstituten

- Marketinginstrument

- Teilweise Vorrausetzung für Geschäftsbeziehungen, z.B. Ausschreibungen

- Langfristig bessere Konditionen für Kredite bei Kapitalgesellschaften

Das Management ist gefordert durch bessere IT Security diese Vorteile auch nutzen zu können! Für fehlende Maßnahmen wie Virusschutz oder Datensicherung haftet komplett das Management/Geschäftsfürung !



Reduzierung von Systemausfällen:

stressfreieres Arbeiten, weniger Überstunden

Verringern von Risiken:

z.B. die Sicherheit von mobilen Geräten birgt ein höheres Risiko des Datenverlusts durch Diebstahl als auch defekte Hardware durch unsachgemäße Handhabung.

Komplexität und Verantwortung meistern:

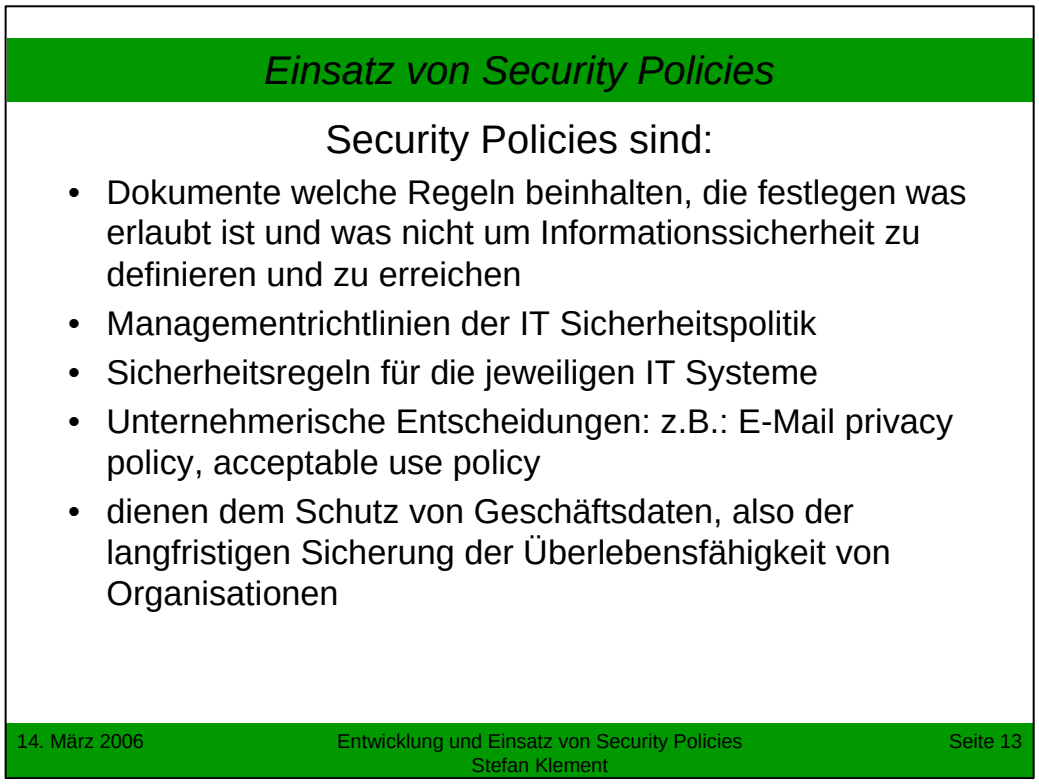
Selbst die Qualität der eigenen Arbeit sicherstellen und dokumentieren.

Mitarbeiter:

Awareness schaffen

Schulungen

Trainings



E-Mail privacy policy:

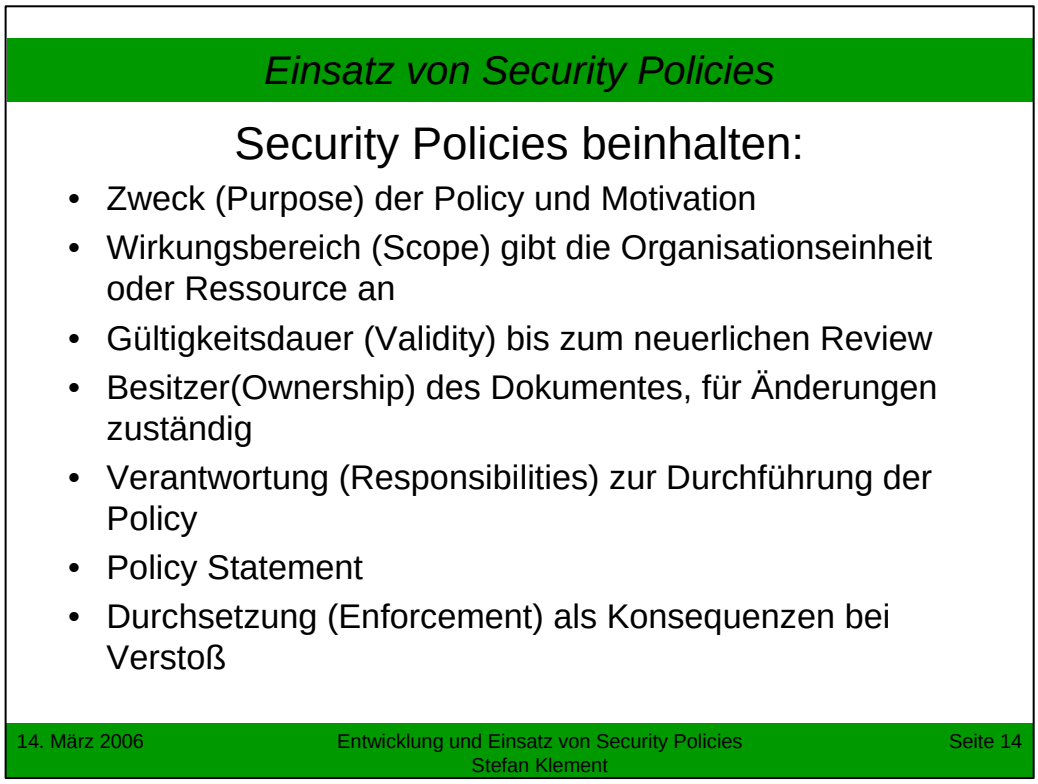
Definiert, wie im Unternehmen mit Emails umgegangen werden muss. Die Policy kann unter anderem erlauben ob private Emails über die Firmen-Emailadresse versendet werden dürfen.

Acceptable Use Policy:

Beschreibt die korrekte Benutzung von IT Equipment und Services. Darf während der Arbeitszeit oder außerhalb das Internet für andere Tätigleiten wie private E-Mails oder Informationssuche verwendet werden?

Sprachgebrauch:

Security Policies (NIST) = Sicherheitsrichtlinien (GSHB)



Zweck (Purpose)

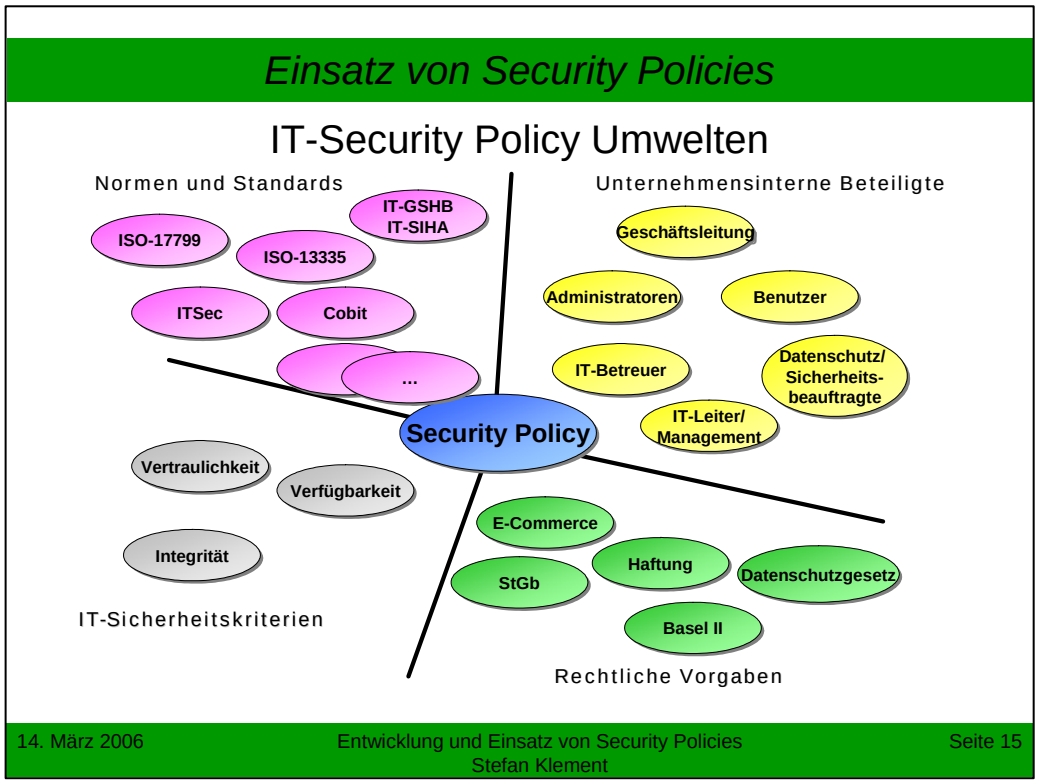
Der eigentliche Zwecks der Policy und Motivation zur Steigerung der Akzeptanz. Dieser erste Punkt des Policy Statements soll dem Leser kurz und einprägsam erklären wozu die Policy verfasst wurde und was damit erreicht werden soll. Dabei soll die Aufmerksamkeit nicht durch lange Erklärungen leiden sondern im Gegenteil die Motivation zum weiter lesen gegeben werden.

Besitzer (Ownership)

Legt fest wer für Änderungen im Dokument zuständig ist. Es sollte nur eine Person Besitzer des Dokumentes sein und dies ändern.

Policy Statement

Die eigentliche Aussage. Das Statement konkretisiert WAS geschützt werden soll, und nicht das technische WIE, dies wird durch die Procedures beschrieben.



Haftung: Sicherheit muss dem Stand der Technik entsprechen, also wirtschaftlich durchführbar sein. Dies ist schwer nachvollziehbar und wird bei Schadensfällen meist durch Sachverständige ermittelt

Datenschutzgesetz 2000: Bundesgesetz über den Schutz personenbezogener Daten

E-Commerce Gesetz: Regelung bestimmter rechtlicher Aspekte des elektronischen Geschäfts- und Rechtsverkehrs

StGB § 118a: Widerrechtlicher Zugriff auf ein Computersystem

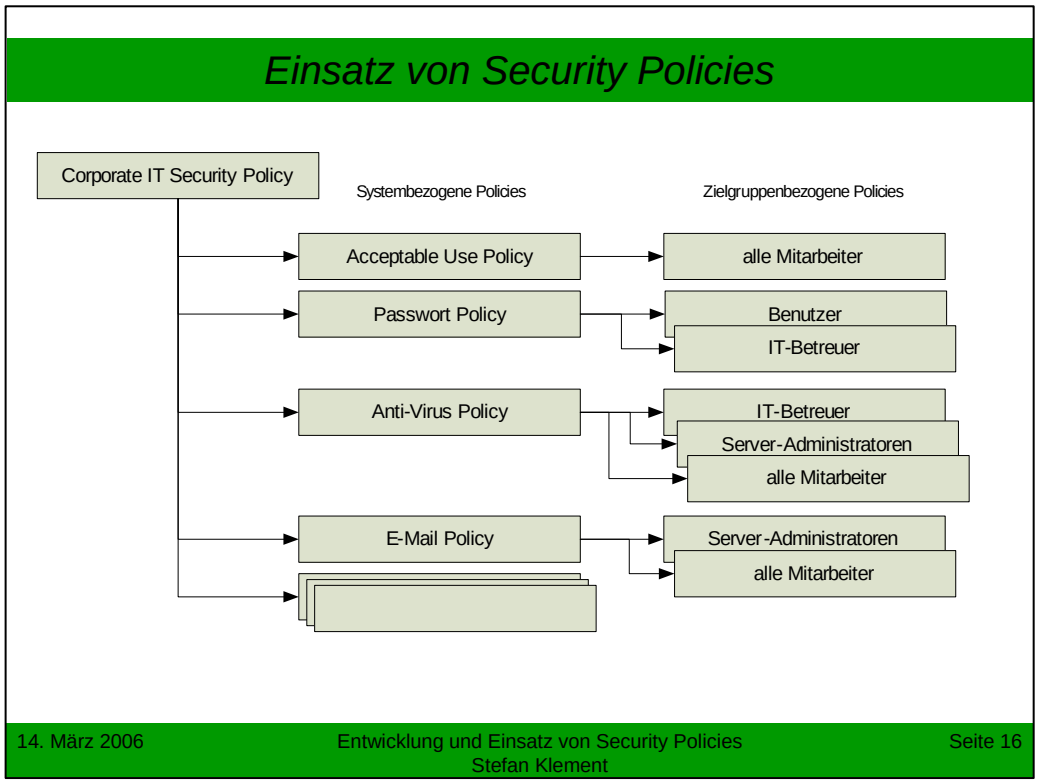
StGB § 119a: Missbräuchliches Abfangen von Daten

StGB § 126a: Datenbeschädigung

StGB § 126b: Störung der Funktionsfähigkeit eines Computersystems

StGB $ 126c: Missbrauch von Computerprogrammen oder Zugangsdaten

Basel II: Basel II bezeichnet die Gesamtheit der Eigenkapitalvorschriften, die vom Basler Ausschuss für Bankenaufsicht in den letzten Jahren vorgeschlagen wurden. Die Regeln werden offiziell in der Europäischen Union Ende 2006 in Kraft treten, finden aber bereits heute in der täglichen Praxis Anwendung. Dabei wird unter anderem das Kreditrisiko anhand eines Ratings bestimmt. Das IT-Sicherheitsniveau eines Unternehmens kann direkte Auswirkungen auf das Rating und somit die Vergabe von Krediten haben.



Die Corporate Security Policy stellt das Basisdokument bei der Entwicklung von Security Policies dar. Sie ist die erste Policy die verfasst werden muss und umfasst folgende Inhalte:

IT-Sicherheitsziele und –strategien

Organisation und Verantwortlichkeiten für IT-Sicherheit

Risikoanalysestrategien, akzeptables Restrisiko und Risikoakzeptanz

Klassifizierung von Daten

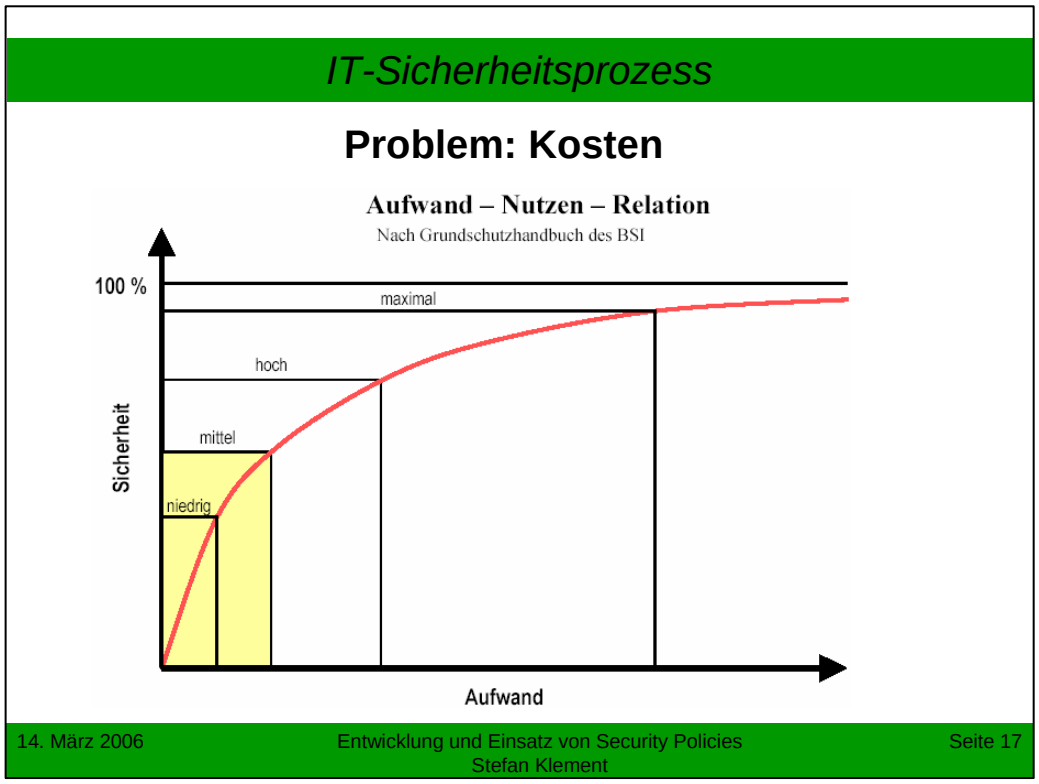
Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung

Aktivitäten zur Überprüfung und Aufrechterhaltung der Sicherheit

Die Anzahl und Detailgenauigkeit der Systembezogenen Security Policies ist stark von der Unternehmensgröße abhängig.

Weitere Policytpen (siehe auch Kapitel 5 für Beispielpolicies):

VPN Security Policy, Remote Access Policy, Backup Policy, Wireless Network Policy, Laptop Security Policy

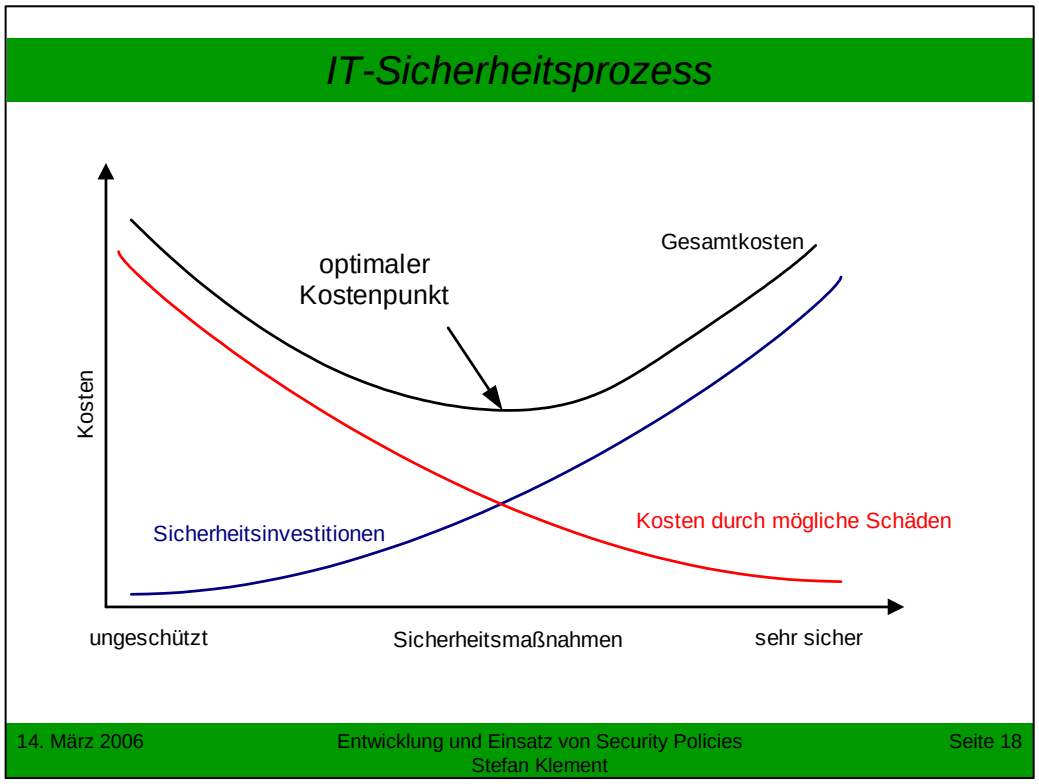


Eine vollkommene, hundertprozentige Sicherheit ist aber nicht zu erreichen. Dies würde bedeuten dass absolut kein Ausfall möglich ist – alleine die Fehlerfreiheit von Software kann nicht bewiesen werden, ebenso wie die Korrektheit eines Prozessordesigns.

Oft befinden sich Unternehmen (besonders kleine und mittlere) im untersten Bereich der Kosten/Nutzen Relation. Als Argument wird meist „kein Budget“ genannt, ohne dass die Entscheider sich bewusst sind, welche Risiken sie eingehen.

Dabei ist der Aufwand, um ein mittleres Sicherheitsniveau zu erreichen im Vergleich zum positiven Nutzen relativ gering. Meist lässt sich durch die IT-Sicherheits „Basics“ ein adäquates Sicherheitsniveau erreichen. Dazu zählen:

- gut konfigurierte Firewall
- durchgängiger Viren/Spywareschutz
- regelmäßige Datensicherung



Oft steigen die Sicherheitsmaßnahmen mit der Größe des Unternehmens, da auch die möglichen Kosten bei Systemausfällen höher sind. Wird bei einem Firmenwachstum nicht in IT-Sicherheit investiert steigen die potentiellen Risiken.

Wenn die Wirtschaftlichkeit von IT-Investitionen eine untergeordnete Rolle spielt gelangen Unternehmen in den Bereich wo die Gesamtkosten wieder steigen. Dies kann durch gesetzliche Vorgaben wie im Gesundheitswesen oder im militärischen Bereich nötig sein. Auch in Unternehmensbranchen wie dem Finanzwesen ist es aus Imagegründen wichtiger Risiken möglichst zu minimieren, unabhängig von den Kosten.

IT-Sicherheitsprozess

Sicherheitshandbücher, Normen und Standards

- österreichisches IT-Sicherheitshandbuch
- deutsches IT-Grundschutzhandbuch
- ISO 17799, ISO 27001
- ISO 13335
- Cobit
- ITSec, Common Criteria

ISO / IEC 17799

Code of Practice for Information Security Management

Stellt eine Sammlung von Maßnahmen bereit die dem Best-practice-Ansatz in der Informationssicherheit genügen.
Unterteilt in 10 Hauptkapitel:

Informationssicherheitspolitik	Computer- und Netzwerkmanagement
Sicherheitsorganisation	Zugangskontrolle
Klassifizierung und Wert-Überwachung	Systementwicklung und Wartung
Sicherheit beim Personal	Geschäftskontinuitätsplanung
Physische und umgebungsbezogene Sicherheit	Erfüllung der Verpflichtungen

Wesentliches Element: Risikomanagement

→Behörden, Unternehmen, nicht für Privatanwender

→IT-Sicherheitsbeauftragter

ISO TR 13335

Guidelines on the Management of IT-Security

Part 1 (1996): Concepts and models for IT Security

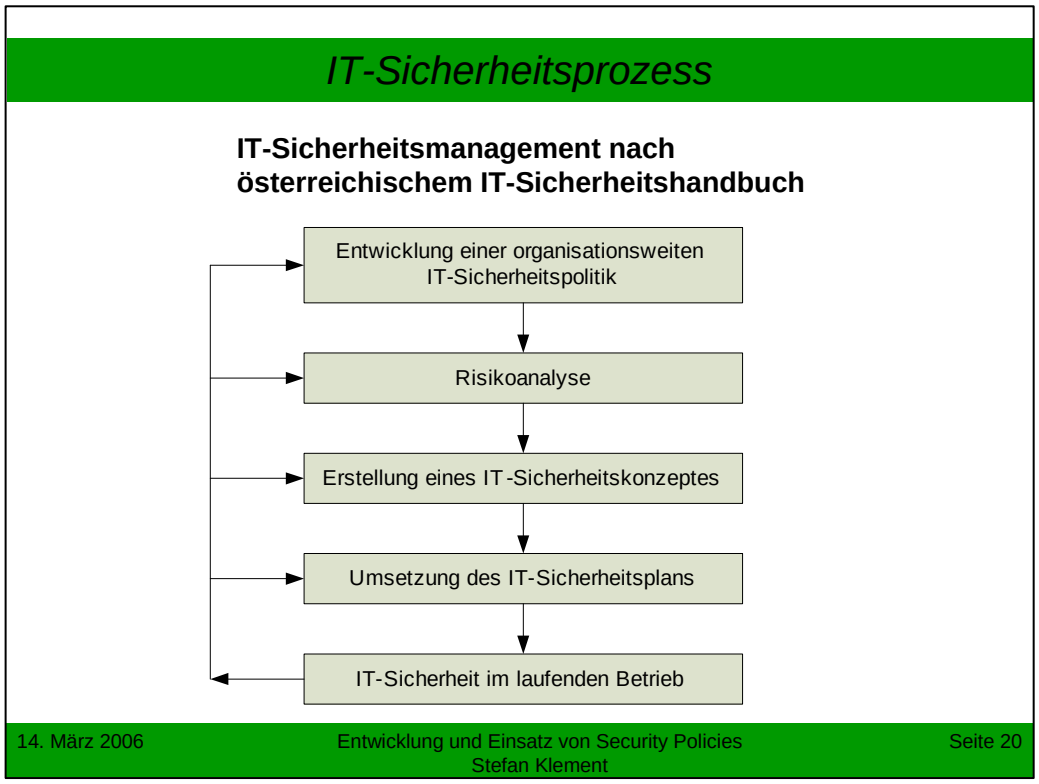
Part 2 (1997): Managing and planning IT Security

Part 3 (1998): Techniques for the management of IT Security

Part 4 (2000): Selection of Safeguards

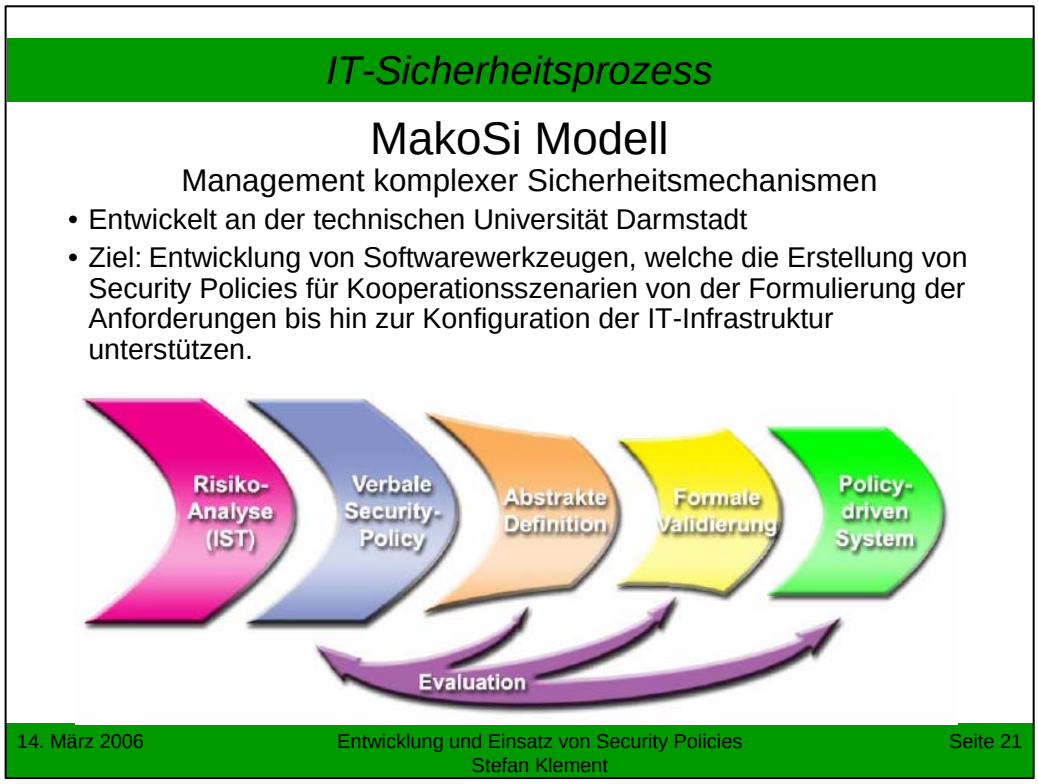
Part 5 (2001): Management Guidance on network security

→Führungskräfte eines Unternehmens zur Planung des IT-Sicherheitsprozesses



Hier steht die **Entwicklung einer organisationsweiten IT-Sicherheitspolitik**, welche auch als Corporate IT Security Policy bezeichnet wird, an erster Stelle und ist somit der auslösende Schritt des Prozesses.
Der Prozess basiert insbesondere auf den "Guidelines on the Management of IT Security (GMITS), ISO/IEC 13335.

Aufgrund der organisationsweiten IT-Sicherheitspolitik wird eine **Risikoanalyse** durchgeführt um Risiken aufzuzeigen und sie auf ein akzeptables Maß zu reduzieren. Dabei können verschiedene Methoden wie die **detaillierte Risikoanalyse,** der **Grundschutzansatz** oder der **kombinierte Ansatz** angewendet werden.

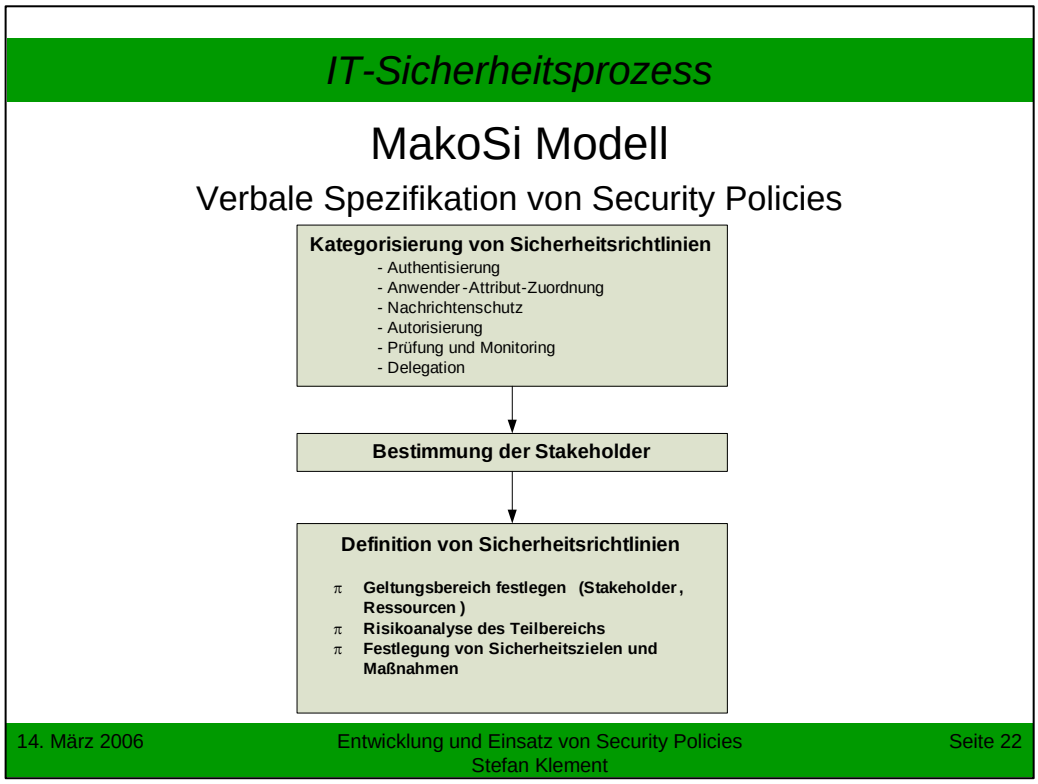


Entwickelt wurde das Modell von Projektpartnern an der technischen Universität Darmstadt und verschiedenen Fraunhofer Instituten.

Das Modell geht davon aus, dass Unternehmen ihre Sicherheitsanforderungen in Form von Security Policies spezifiziert, welche für das ganze Unternehmen, Unternehmensteile oder Kooperationen gelten.

Ziel des Vorgehensmodells ist es, domänenübergreifende Zusammenarbeit zu realisieren und die beteiligten Stakeholder von der Spezifikation bis zur Implementierung zu unterstützen.

Eine Domäne, im Makosi Modell auch Security Policy Domain genannt, ist dabei eine Unterteilung um Ressourcen und Anwender bestimmten Gruppen mit ähnlichen Sicherheitsanforderungen zuzuordnen.

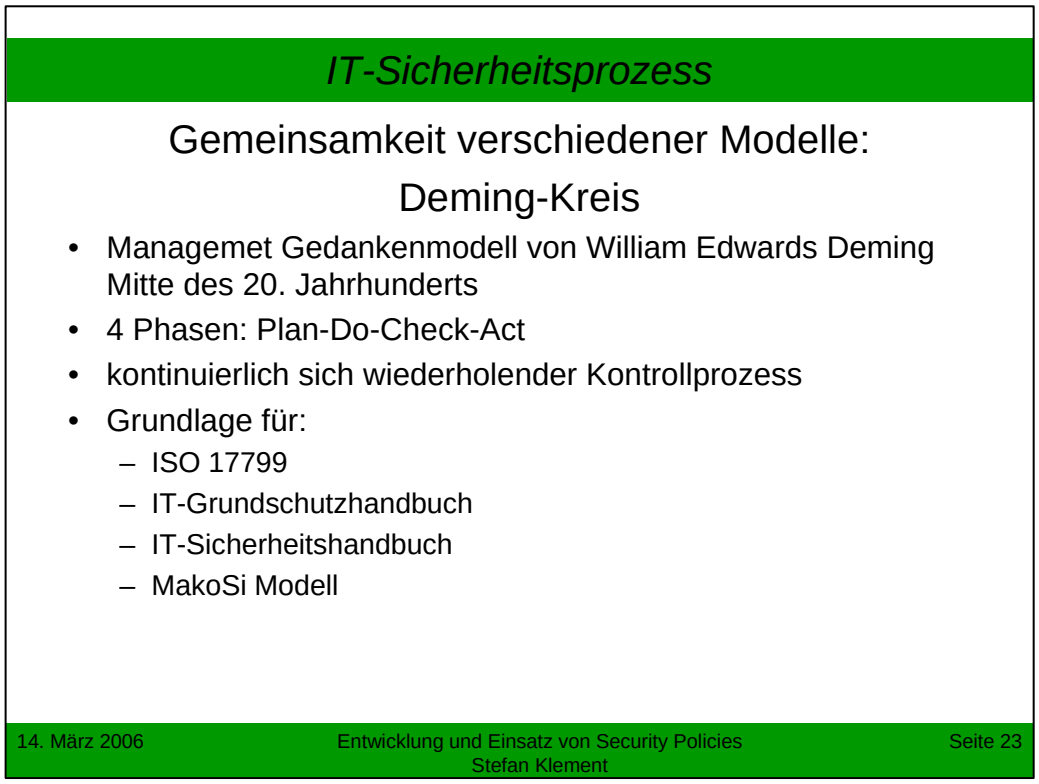


Zu Beginn steht die **Kategorisierung anhand der Sicherheitsmechanismen**:

- Authentisierung – Definition der Authentisierungsprotokolle
- Anwender-Attribut-Zuordnung – Festlegung, über welche Sicherheitsattribute ein authentifizierte Anwender zu verfügen hat
- Nachrichtenschutz – Definition von Maßnahmen zum Schutz auszutauschender Geschäftsdaten, d. h. Authentizität, Vertraulichkeit, Integrität etc.
- Autorisierung – Definition, welche Anwender bzw. Anwendungen welche Zugriffrechte auf Ressourcen in der verteilten Umgebung haben
- Prüfung und Monitoring – Festlegung, welche Events zu protokollieren sind
- Delegation – Festlegung, ob und wie Benutzerprivilegien an Systeme weitergereicht bzw. vererbt werden.

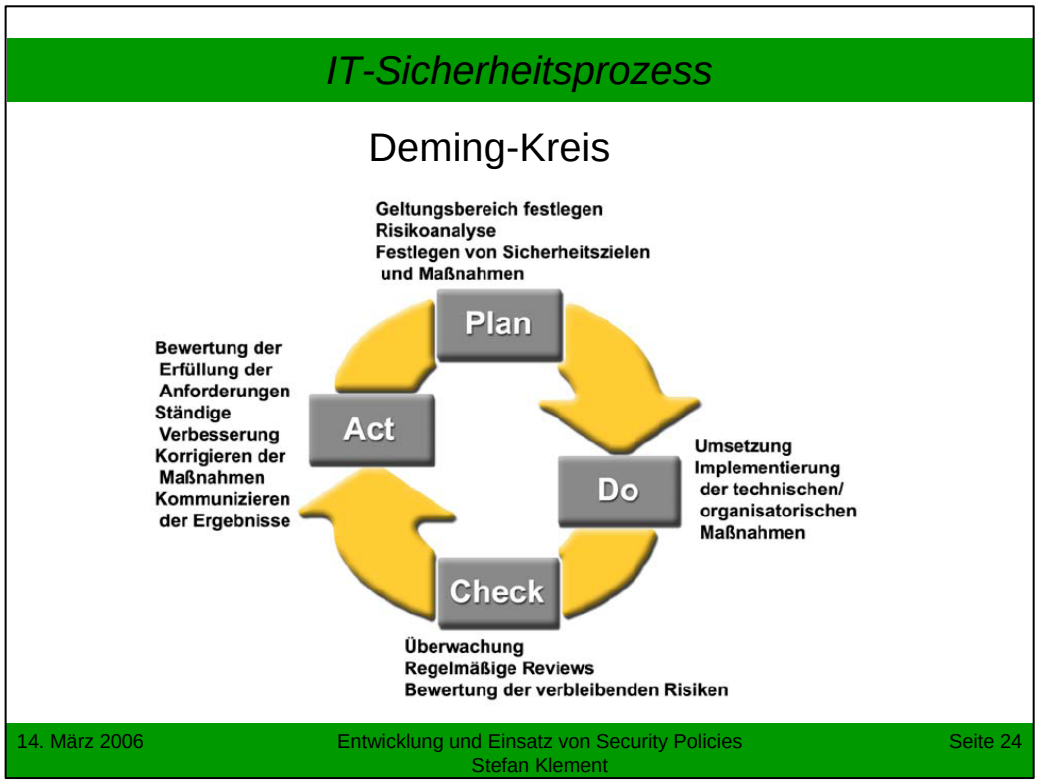
Die Definition der Sicherheitsrichtlinien soll unter Beachtung folgender Punkte erfolgen:

- **Angestrebtes Sicherheitsniveau**
- **Beschaffungskosten**
- **Administrations- und Wartungsaufwand**
- **Benutzerfreundlichkeit**
- **Skalierbarkeit**
- **Investitionssicherheit**



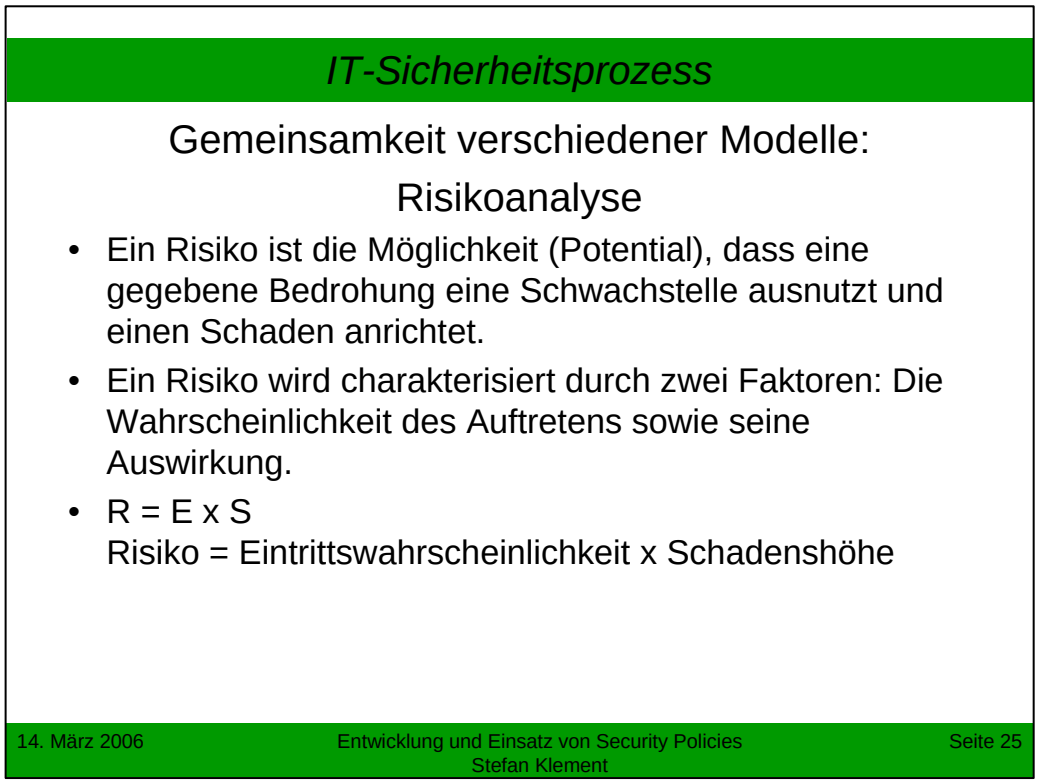
William Edwards Deming (* 14. Oktober 1900 in Sioux City, Iowa; † 20. Dezember 1993 in Washington D.C.) war ein US-amerikanischer Physiker, Statistiker sowie Wirtschaftspionier im Bereich des Qualitätsmanagements. Er entwickelte ab den 1940er-Jahren die prozessorientierte Sicht auf die Tätigkeiten eines Unternehmens, die später auch Eingang in die diversen Qualitätsnormen und Qualitätsmanagementlehren fand.

Besonders verbreitet sind die Ideen von Deming in Japan, wo sie ab Mitte des letzten Jahrhunderts zur deutlichen Qulitätssteigerung der Arbeitsprozesse geführt haben.

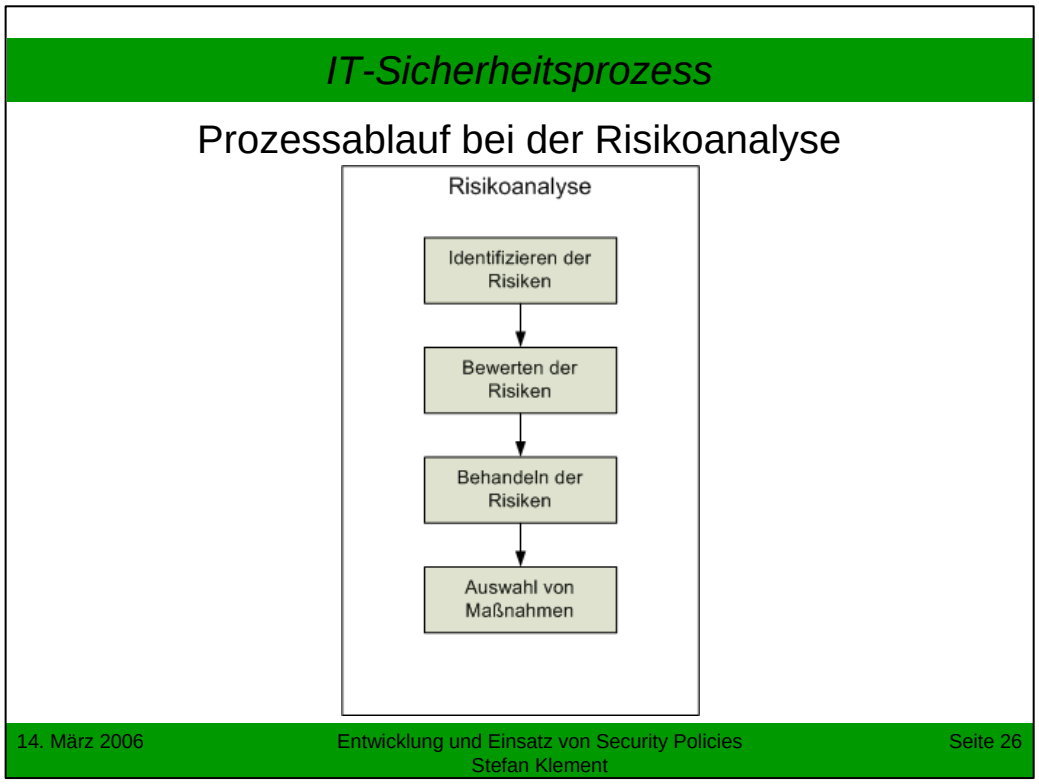


Sowohl das IT-Sicherheitshandbuch als auch das Grundschutzhandbuch können als Ausgangspunkt für einen solchen PDCA-Zyklus gesehen werden. Sie bilden die einzelnen Phasen von der Risikoanalyse über die Maßnahmen zur Überwachung und Restrisiko bis zur Aufrechterhaltung im laufenden Betrieb genau ab.

Im BS 7799-2 wird aufgrund des PDCA-Zyklus eine Erhöhung des Informations-sicherheitsniveaus angestrebt.
Im Unterschied zu den Sicherheitshandbüchern ist beim BS 7799-2 der Fokus auf die stetige Verbesserung des durchlaufenen Zyklus gelegt.
Aufgrund des BS 7799-2 wurde beim Makosi-Modell der Deming-Kreis zur Definition von Security-Policies verwendet, mit besonderem Bezug auf die Plan Phase.

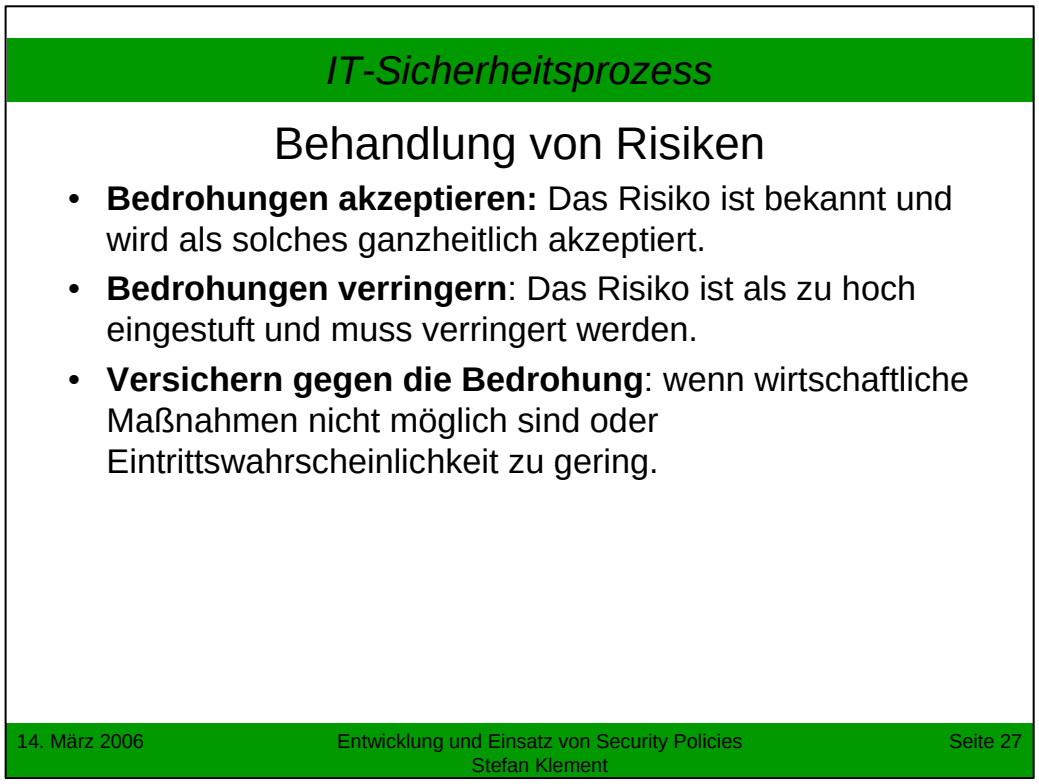


Für adäquate IT Security Policies ist das Risikomanagement unumgänglich, da erst durch bestimmen der Risiken und Bedrohungen geeignete Maßnahmen entworfen und eingeleitet werden können. Die Risikoanalyse ist eigentlich ein Managementwerkzeug, um Entscheidungen begründet treffen zu können. Dabei muss die Risikoanalyse immer zu Beginn eines IT-Sicherheitsmanagementprozesses stehen.



Im ersten Schritt werden die **Risiken identifiziert,** welche sich durch verschiedene Bedrohungen ergeben. Eine vollständige Aufstellung aller Bedrohungen für alle IT-Systeme wird selten möglich sein, und ist meist auch zu umfangreich. Hilfestellung hierbei geben Gefährdungskataloge wir aus dem Grundschutzhandbuch welche die wichtigsten Bedrohungsarten klassifizieren und somit eine Zuteilung zu den IT-Systemen einfacher machen.

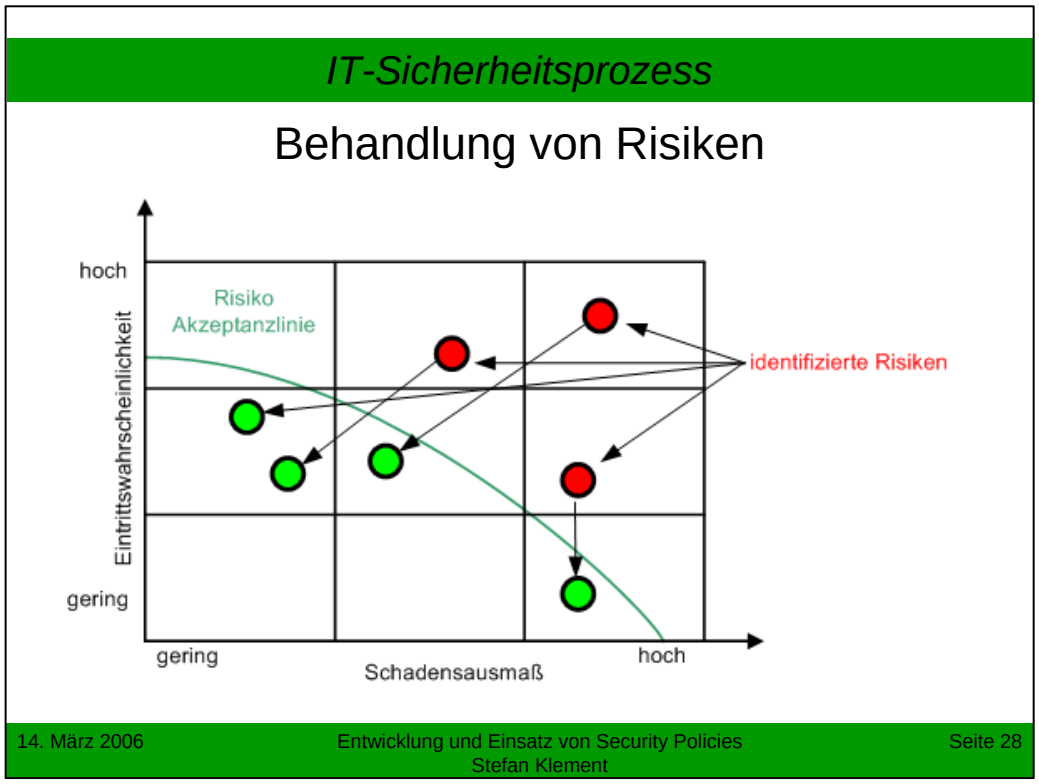
Beim **Bewerten der Risiken** gibt es mehrere Methoden, die bekanntesten sind die **Detaillierte Risikoanalyse**, der **Grundschutzansatz** und der **kombinierte Ansatz.** Dabei geht es in jeder Methode darum die Werte des Unternehmens festzustellen, das Resultat wenn eine Bedrohung eintritt und den damit verbundenen Verlust. Dies können Datenverlust, nicht verfügbare IT-Systeme, unautorisierter Zugriff oder immaterielle Werte wie Imageverlust oder reduziertes Kundenvertrauen sein.



Bedrohungen akzeptieren: Auch diese Entscheidung muss schriftlich festgehalten werden.

Bedrohungen verringern: Da R = E x S kann entweder die Eintrittswahrscheinlichkeit (z.B. durch ausfallsichere Hardware) oder die entstehende Schadenshöhe (z.B. durch angemessene Datensicherung) reduziert werden.

Versichern gegen die Bedrohung:
Hierzu zählen unter anderem Feuer- und Diebstahlversicherungen oder Betriebsausfall-versicherungen.



Die identifizierten Risiken welche sich über der gedachten Risiko Akzeptanzlinie befinden müssen durch verschiedene Prozesse in den „grünen“ Bereich übergeführt werden. Dies kann durch eine der zuerst aufgeführten Risikobehandlungen erreicht werden.

Vertikale Verschiebung = Verringerung der Eintrittswahrscheinlichkeit
z.B. durch redundante Hardwaresysteme, gut geschützte Netzwerke, passende Security Policies

Horizontale Verschiebung = Verringerung des Schadensausmaßes

z.B. durch Datensicherungen (ein Speichermedium wird immer noch mit gleicher Wahrscheinlichkeit defekt, aber im Schadensfalls könne die Daten mit einigem Zeitverlust wiederhergestellt werden), Hardware-Supportverträge, Versicherungen

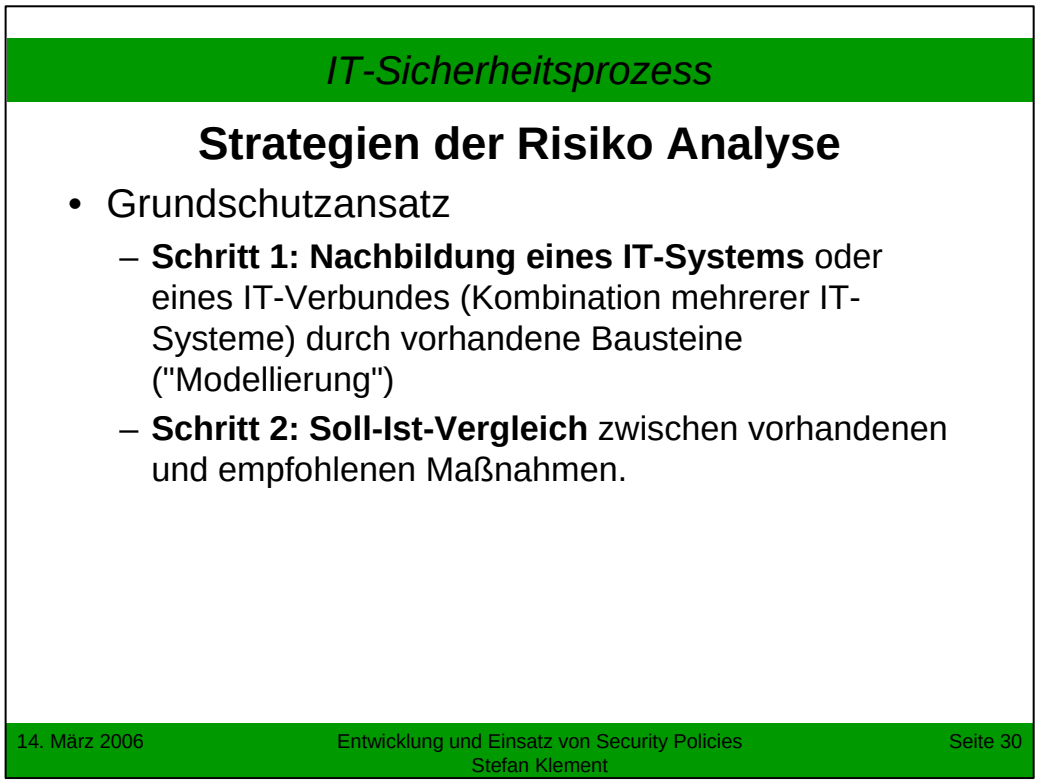
Schwierig ist die „richtige“ Auswahl von Maßnahmen um die geforderten Ziele zu erreichen! Einen umfangreichen Maßnahmenkatalog bietet das deutsche Grundschutzhandbuch [BSI05]

Strategien der Risiko Analyse

- Detaillierte Risikoanalyse:
  - Großer Aufwand – Wochen bis Monate
  - Genaue Wertanalyse der bedrohten Objekte
  - Ermitteln und bewerten der Einzelrisiken und des Gesamtrisikos
- Grundschutzansatz
  - Ziel ist es, den Aufwand für die Erstellung eines IT-Sicherheitskonzeptes angemessen zu begrenzen.
  - Gefahren werden kategorisiert, keine detaillierte Risikoanalyse
  - Auswahl auf der Basis vorgegebener Kataloge. (IT-Grundschutzhandbuches des BSI)

Als erste Strategie wird immer der Grundschutzansatz empfohlen, um rasch auf ein mittleres Sicherheitsniveau zu kommen. Dies wird sowohl im österreichischen IT-Sicherheitshandbuch als auch im deutschen Grundschutzhandbuch in dieser Form angewandt.

Eine detaillierte Risikoanalyse mit entsprechend großem Aufwand wird in KMUs selten umgesetzt. Ausnahmen sind Unternehmen welche z.B. einen 24x7 Betrieb mit wenigen und kurzen Ausfallzeiten gewährleisten müssen.



Der Grundschutzansatz wird besonders unter folgenden Umständen empfohlen [Sihb04]:

•Wenn feststeht, dass im betrachteten Bereich nur IT-Systeme mit niedrigem oder mittlerem Schutzbedarf zum Einsatz kommen.

•Falls in einem Bereich (IT-System, Abteilung,...) noch keine oder offensichtlich zu schwache Sicherheitsmaßnahmen vorhanden sind, kann die Realisierung von Grundschutzmaßnahmen dazu beitragen, rasch ein relativ gutes Niveau an IT Sicherheit zu erreichen.

•Als Teil eines umfassenden Risikoanalysekonzeptes ("kombinierter Ansatz")

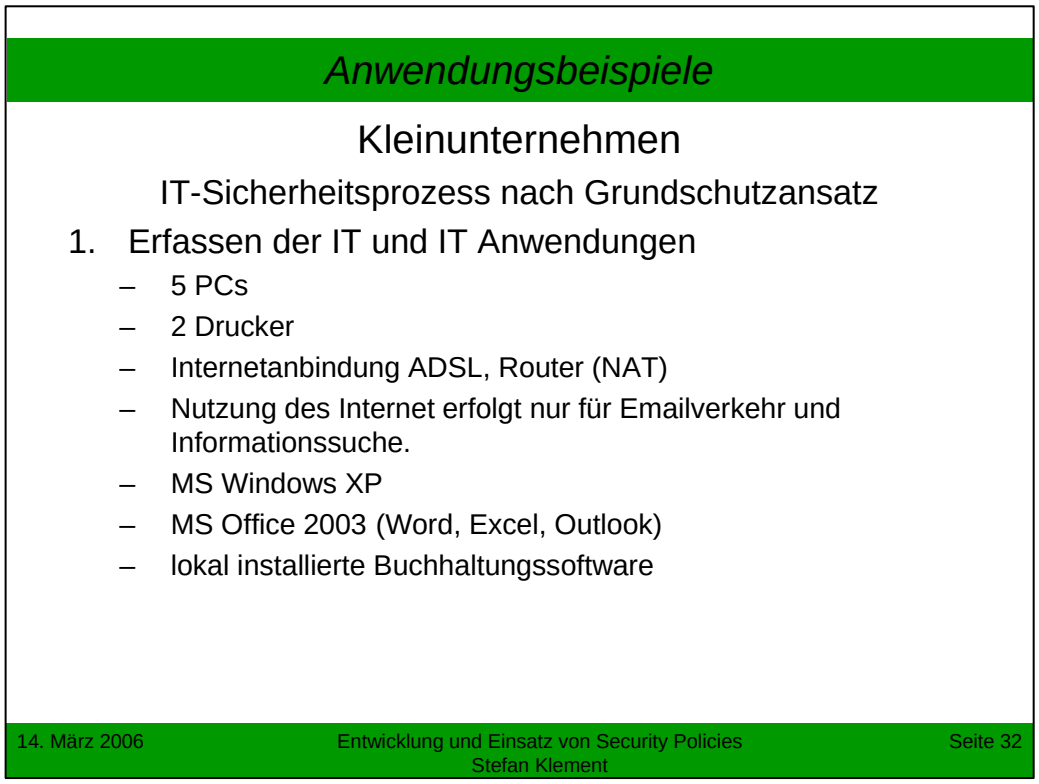
Schicht 1 umfasst die **übergreifenden IT-Sicherheitsaspekte**, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. (unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Virenschutzkonzept)

Schicht 2 befasst sich mit den **baulich-technischen Gegebenheiten**, in der Aspekte der infrastrukturellen Sicherheit zusammengeführt werden. (Gebäude, Serverraum, Schutzschrank, häuslicher Arbeitsplatz)

Schicht 3 betrifft die einzelnen **IT-Systeme** des IT-Verbunds. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. (TK-Anlage, Laptop, Clients)

Schicht 4 betrachtet die **Vernetzungsaspekte** der IT-Systeme, die sich nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. (Heterogene Netze, Modems, Remote Access)

Schicht 5 schließlich beschäftigt sich mit den eigentlichen **IT-Anwendungen**, die im IT-Verbund genutzt werden. (E-Mail, Webserver, Faxserver, Datenbanken)



Bei der Erfassung werden die IT Komponenten durch vorhandene Bausteine im IT-Grundschutzhandbuch modelliert, oder durch Kombination mehrerer IT-Systeme zu einem IT-Verbund.

Nur so sind danach pauschalierte Maßnahmen aus dem Maßnahmenkatalog auszuwählen und umzusetzen.

Dies funktioniert bei den meisten Unternehmen welche Informations Technologie als Prozessunterstützung verwenden (Buchaltung, Angebote,..). Bei spezialisierten IT Unternehmen wird oft eine genaue Analyse notwendig sein um alle Komponenten und deren Wichtigkeit zu erfassen.

Anwendungsbeispiele

Kleinunternehmen

2. Schutzbedarfsfeststellung

Schutzbedarfskategorien	
niedrig bis mittel	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Es wird ermittelt, dass nur Schutzbedarfskategorien „niedrig bis mittel“ existieren. Dies spricht für den Einsatz des Grundschutzansatzes.

Bei ermittelten Schutzbedarfskategorien „sehr hoch“ wird die detaillierte Risikoanalyse empfohlen, da man davon ausgehen kann dass vorgefertigte Bausteine das geforderte Sicherheitsniveau nicht erreichen können.

Dies wäre der kombinierte Ansatz, welcher beide Strategien und ihre Vorteile vereint. Durch die Grundschutzanalyse wird Zeit und Kosten gespart, durch die detaillierte Risikoanalyse werden hohe Sicherheitsrisiken reduziert.

Anwendungsbeispiele

Kleinunternehmen

3. Basis-Sicherheitscheck nach Grundschutzhandbuch Auswahl der vorhandenen Bausteine:
   - Übergeordnete Aspekte
     - B 1.4 Datensicherungskonzept
     - B 1.6 Computer-Viren-Schutzkonzept
     - B 1.13 IT-Sicherheitssensibilisierung und –schulung
   - IT-Systeme
     - B 3.209 Client unter Windows XP
     - B 3.301 Sicherheitsgateway (Firewall)
   - IT-Anwendungen
     - B 5.3 E-Mail
4. Soll-Ist Vergleich zwischen vorhandenen und empfohlenen Maßnahmen

Nach BSI-Grundschutzhandbuch werden folgende fünf große Bausteine definiert:

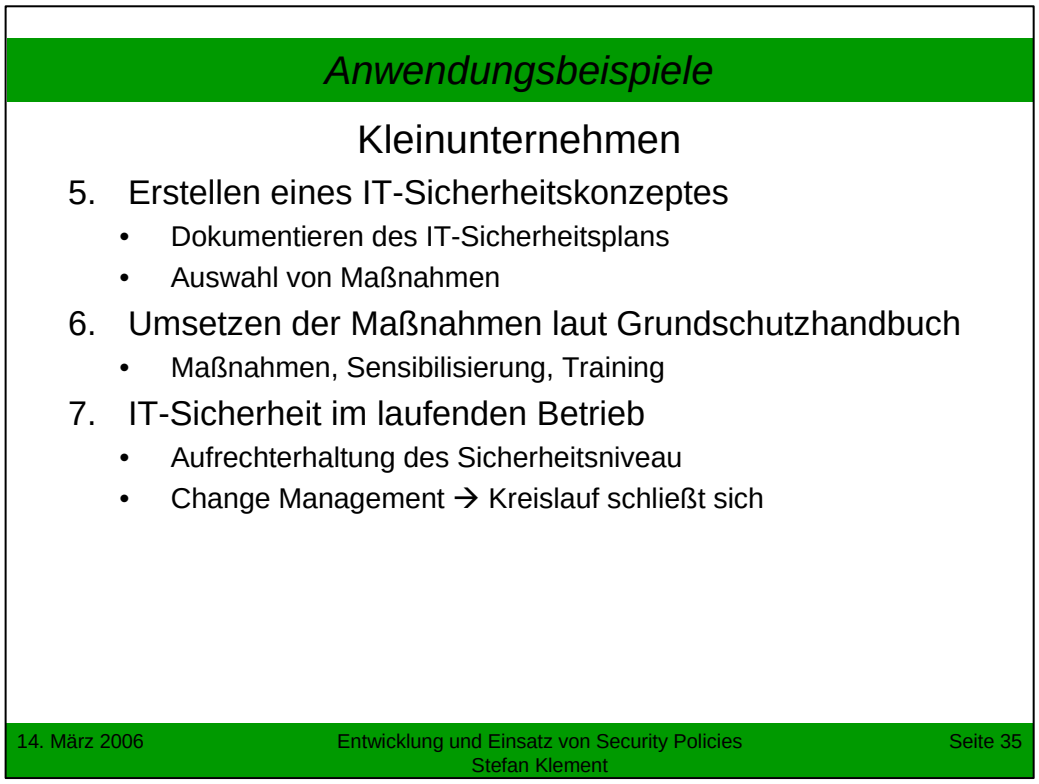
•Übergreifende Aspekte: Personal, Organisation,..

•Infrastruktur: Stromversorgung, WAN-Provider,..

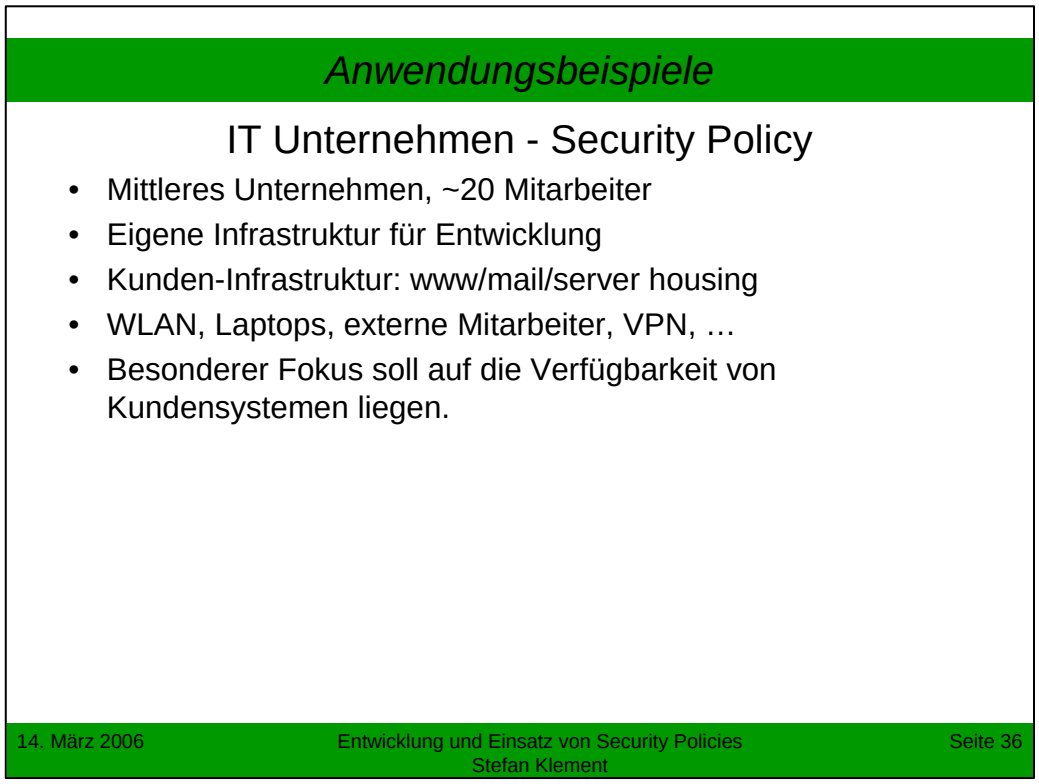
•IT-Systeme: TK-Anlage, DB-Server,..

•Netze: LAN, WAN, Remote Access,..

•IT-Anwendungen: Buchhaltung, Datenbanken, E-Mail,..

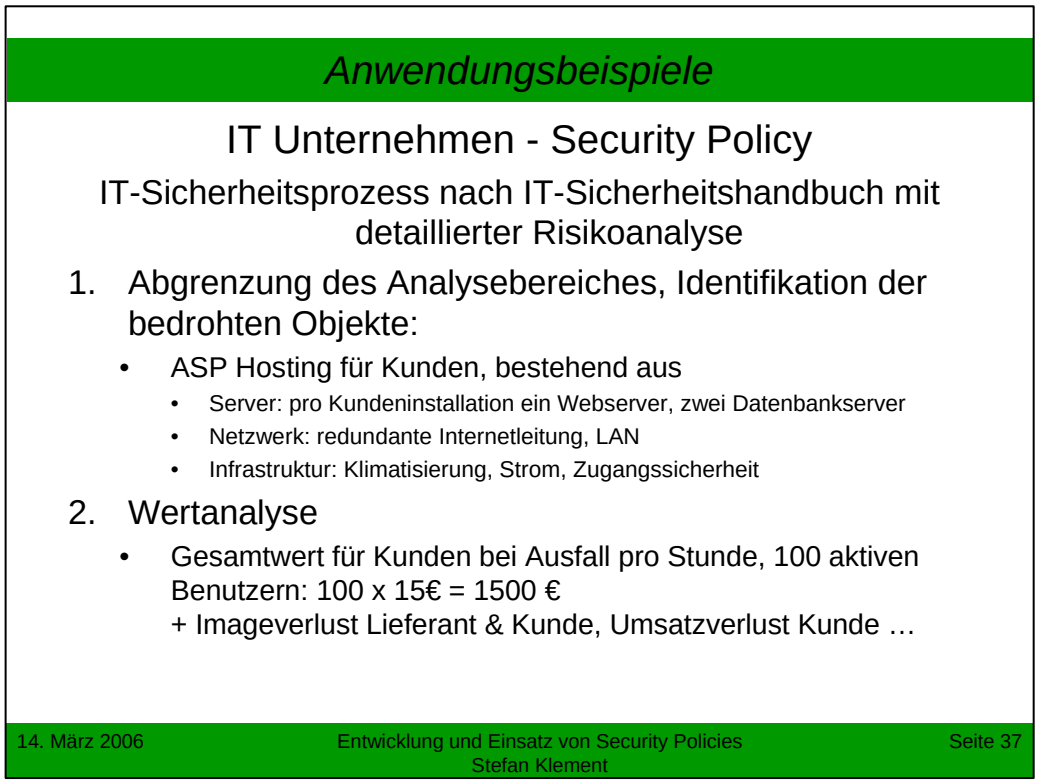


Das Grundschutzhandbuch bietet auf über 2500 Seiten Maßnahmen zu den kategorisierten Gefährdungskatalogen an. Es wird regelmäßig überarbeitet, kann aber der schnellen Entwicklung neuer Technologien nicht sofort folgen. So ist unter anderem für Voice over IP noch keine Kategorisierung erfolgt.



Das besondere bei diesem Beispiel ist, dass IT Infrastruktur nicht nur unterstützend sondern als Unternehmenswert gesehen wird. Kommt es zu längeren Ausfällen oder Datenverlust hat dies sofortige Wirkung auf den Output des Unternehmens.

Jeder Ausfall, auch wenn er noch so kurz ist, schadet dem Image. Hier muss die Gratwanderung zwischen bezahlbaren redundanten Systemen und Ausfallsicherheit gelingen.



Schritt 2: Wertanalyse

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt. Die Wertanalyse umfasst im Einzelnen:

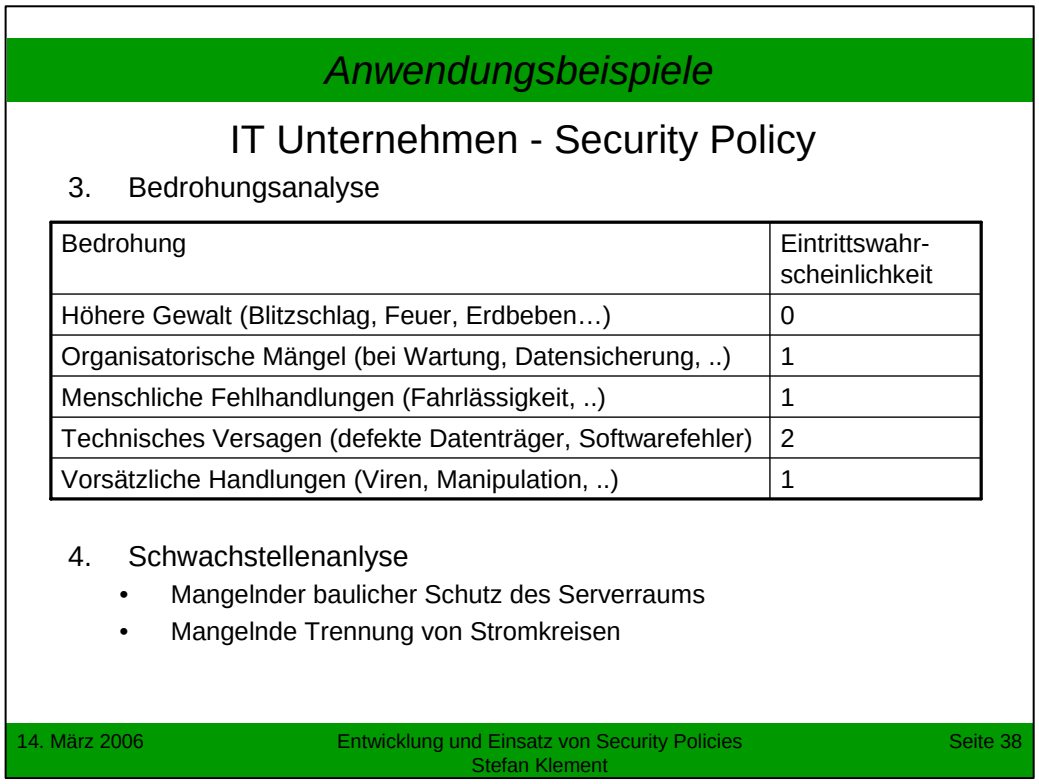
die Festlegung der Bewertungsbasis für Sachwerte

die Festlegung der Bewertungsbasis für immaterielle Werte

die Ermittlung der Abhängigkeiten zwischen den Objekten

die Bewertung der bedrohten Objekte

Als Basis für die Wertanalyse zählen zum Beispiel Verträge mit Kunden, Pönalen oder Reaktionszeiten .



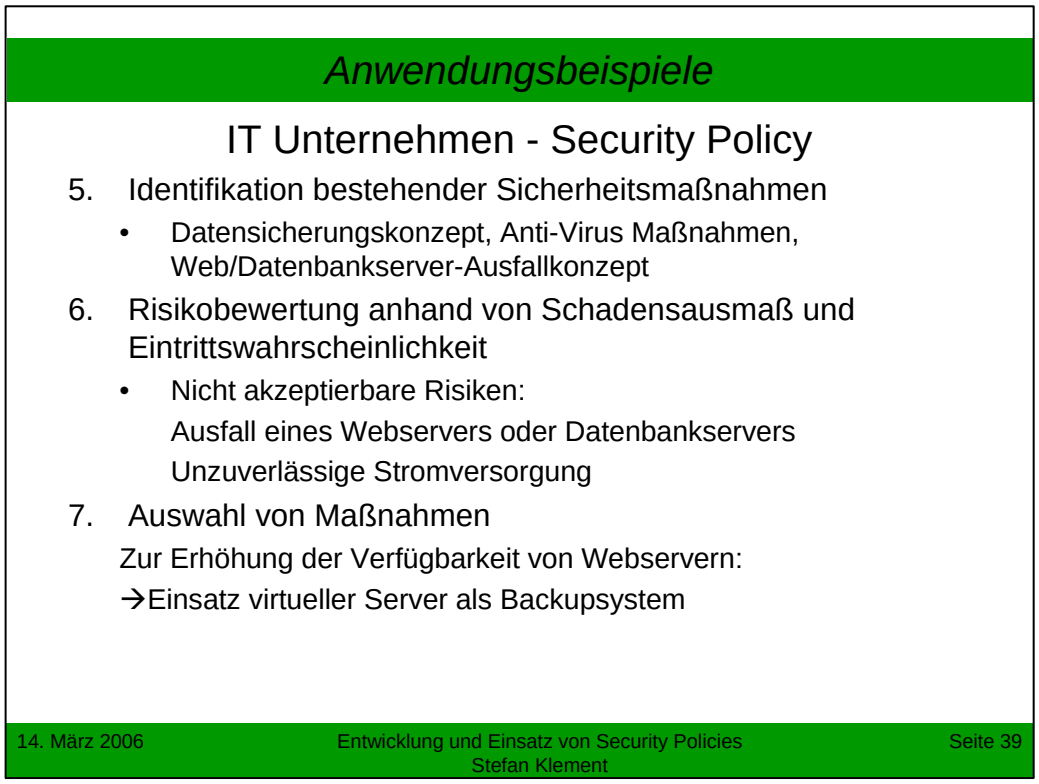
Als Einteilungsschema für die Eintrittswahrscheinlichkeit bewährt haben sich hier etwa drei- bis fünfteilige Skalen, wie beispielsweise:

- 4: sehr häufig
- 3: häufig
- 2: mittel
- 1: selten
- 0: sehr selten

Diese allgemeinen Bedeutungen der Skalenwerte sind für den spezifischen Anwendungsbereich zu konkretisieren. Im Allgemeinen werden sie in "Anzahl pro Zeiteinheit" angegeben. Sie sollten so festgelegt werden, dass die Bedeutung der Ziffern von 0 bis 4 gleichmäßig zunimmt.
Beispiel:

- 4: einmal pro Minute
- 3: einmal pro Stunde
- 2: einmal pro Tag
- 1: einmal pro Monat
- 0: einmal im Jahr

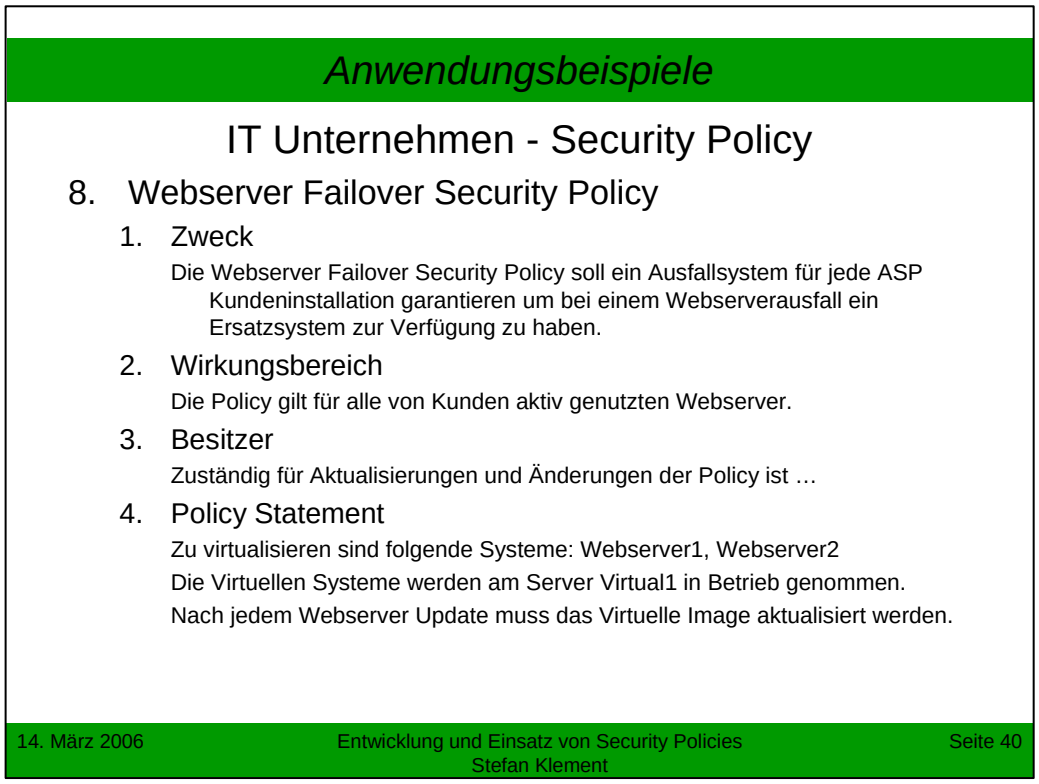
Es kann durchaus sinnvoll oder sogar erforderlich sein, für verschiedene Anwendungs-bereiche unterschiedliche Auslegungen der Werteskala zu definieren.



Der Einsatz virtueller Server wurde aus folgenden Gründen gewählt:

- Kosteneffektiv und wirtschaftlich, keine Anschaffung von Hardware notwendig da ein Server für Virtualisierung bereits besteht.
- Know-How ist vorhanden
- In einem kurzen Zeitraum (einige Wochen) umsetzbar

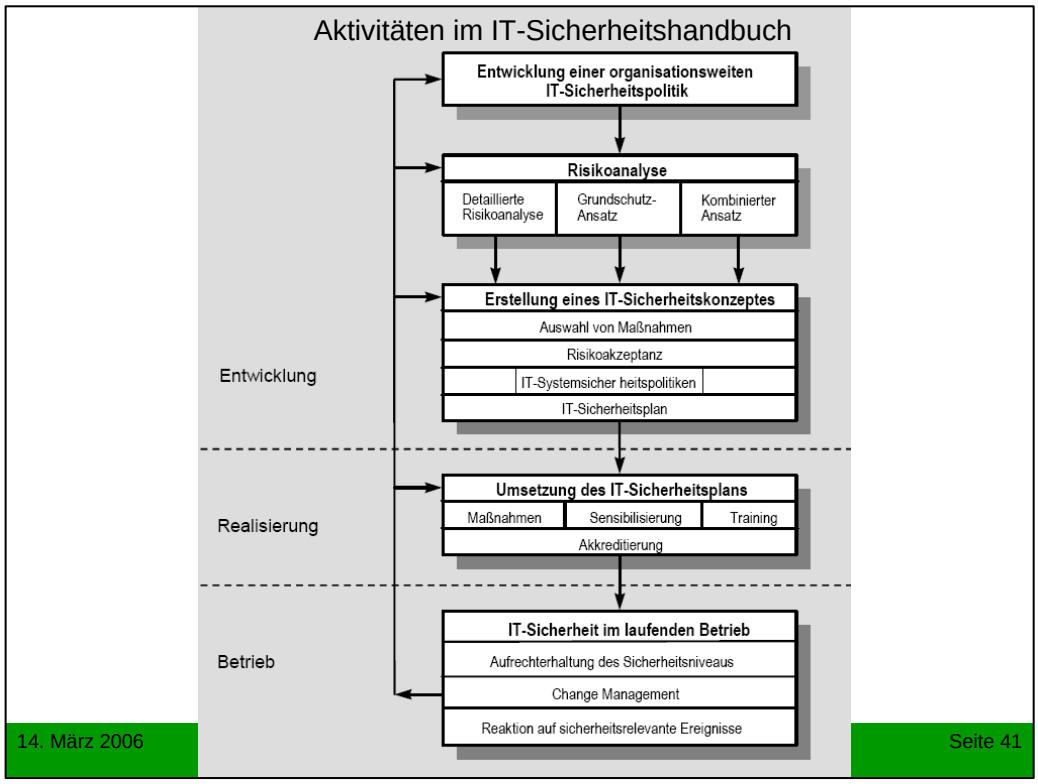
Verwendet werden virtuelle Server in diesem Fall für die externen Webserver. Dazu muss der Inhalt der aktiven Servers (wie HTML oder PHP Files) am virtuellen abgelegt werden. Man muss auch dafür sorgen, dass Aktualisierungen des Echtsystems auch am virtuellen Ausfallsystem durchgeführt werden.



Genaue Details, wie das Policy Statement umzusetzen ist, werden in den Policy Procedures beschrieben.

In diesem Fall z.B., mit welchen Parametern das virtuelle Image erstellt werden muss, wie die Virtualisierungssoftware korrekt verwendet werden soll.

Virtualisierung benötigt natürlich mehr Systemressourcen als ein Betriebssystem, welches direkt auf der Hardware läuft. Besonders bei Installationen wo keine dauernde, hohe Auslastung vorhanden ist macht Virtualisierung aus Effizienzgründen Sinn. Auch bei Testumgebungen ist Virtualisierung von Vorteil, da Virtuelle Images im Vergleich zu einem kompletten Serversetup schneller und kostengünstiger verwendet werden können.



Diese Grafik zeigt die Aktivitäten im Rahmen des IT-Sicherheitsmanagements wie sie im Österreichischen IT-Sicherheitshandbuch beschrieben sind. Das Handbuch geht auf die einzelnen Aktivitäten und deren eventuelle Rückkopplungen genau ein. Im Unterschied zum deutschen Grundschutzhandbuch werden keine Maßnahmenkataloge angeführt.

Im Bereich der öffentlichen Verwaltung ist die Etablierung dieses Prozesses auf Ressortebene verbindlich.

Dies ist noch einmal der Ablauf wie er in den Beispielen der Folien bis jetzt behandelt wurde. Er dient als Überblick und Zusammenfassung der Abläufe.

Zusammenfassung

- eine Security Policy wird als schriftliches Dokument erstellt und bildet die Grundlage des IT-Sicherheitsmanagements
- Security Policies legen Leitlinien fest, schreiben aber keine Implementierungen vor
- Policies werden offiziell in Kraft gesetzt und verabschiedet
- Jeder Mitarbeiter muss Kenntnis über die wichtigsten Inhalte der für ihn zutreffenden Security Policies haben
- Policies sollten so einfach wie mögliche gehalten werden, komplizierte und lange Dokumente wirken eher abschreckend

Vielen Dank für ihre Aufmerksamkeit!

Stefan Klement
klement@ebit.at

Diese Folie kann vom Vortragenden angepasst werden.

7 Zusammenfassung

Die in der Literatur vorkommenden Modelle zur Umsetzung von IT-Sicherheit zeigen, dass dies ein komplexer Prozessablauf ist. Kern ist jeweils die Corporate IT Security Policy mit ihren systembezogenen Policies für die einzelnen Bereiche. Eine wichtige Basisvorrausetzung zur erfolgreichen Umsetzung von Security Policies ist die baldige, klare Definition des IT-Sicherheitsprozesses und die personellen Zuständigkeiten. Damit ist eine Unterstützung der Geschäftsführung oder des oberen Managements wichtig, um die benötigte Akzeptanz für IT-Sicherheit und die Security Policies zu erreichen.

Eine Herausforderung, und gesetzlich nicht geregelt oder vorgeschrieben, ist beim IT Security Prozess die Entscheidung, wie viel in IT Sicherheit investiert werden soll (muss), um die Geschäftstätigkeit zu sichern. Hierzu gibt es keine genauen Regeln oder Gesetze. Klar ist momentan nur (durch verschiedene Gerichtsurteile), dass die Geschäftsführung für IT Sicherheit nach „aktuellem Stand der Technik“ zu sorgen hat. Dies betrifft heute Antivirussoftware, Firewall und Datensicherung. Viele weitere Maßnahmen, wie auch das Erstellen detaillierter IT Security Policies, würden die IT Sicherheit erhöhen, scheitern aber oft am Aufwand oder den Kosten.

8 Abbildungs- und Tabellenverzeichnis

9 Glossar

Availability	Verfügbarkeit
Confidentiality	Vertraulichkeit, Schutz vor unautorisiertem Zugriff.
Corporate IT Security Policy	Unternehmensweite IT Sicherheitsrichtlinie, von Managementebene beauftragt und in Kraft gesetzt.
Detection	Angriffserkennung und Reaktion.
Enforcement	Durchsetzung einer Policy indem für Verstöße (beabsichtigte oder grob fahrlässige Handlungen) Strafaktionen definiert werden.
Integrity	Integrität
Intrusion Detection System	Ein Programm das der Erkennung von Angriffen auf ein Computersystem oder Computernetz dient.
KMU	Kleine und mittlere Unternehmen ist die Bezeichnung für Unternehmen des Mittelstandes.
Malware	Bösartiger Code, Überbegriff für Viren, Würmer und Trojanische Pferde
Prevention	Prävention, Vorsorge gegen mögliche Sicherheitsschwachstellen und Angriffe.
Recovery	Wiederherstellung nach einem Sicherheitsvorfall.
Return On Investment	Der ROI ist eine Renditekennzahl für die Gesamtkapitalrentabilität. Er errechnet sich als Quotient aus dem Periodengewinn und Kapitaleinsatz.
Security Objectives	IT - Sicherheitskriterien
Security Policy	IT-Sicherheitspolitik, IT-Sicherheitsleitlinie. Dokumente welche Regeln enthalten, die festlegen was erlaubt ist und was nicht um Informationssicherheit zu definieren.
Social Engineering	Bezeichnet das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher Kontakte.

10 Literatur

[And02]	Andress, Mandy, „*Surviving Security: How to Integrate People, Process, and Technology*“, Sams Publishing, Indianapolis, 2002
[Bit05]	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), Leitfaden „*Matrix der Haftungsrisiken*“, 10. März 2005, http://www.bitkom.org/de/themen_gremien/18173_31034.aspx
[Bsi05]	Bundesamt für Sicherheit in der Informationstechnik, „*IT-Grundschutzhandbuch*“, 2004, http://www.bsi.bund.de/gshb/index.htm
[Bsi05/1]	Bundesamt für Sicherheit in der Informationstechnik, „*IT-Grundschutzhandbuch*“, 2004, G 5.23 Computer-Viren, http://www.bsi.bund.de/gshb/deutsch/g/g05023.html
[Bsi05/2]	Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.0“, Dezember 2005, http://www.bsi.bund.de/literat/bsi_standard/index.htm
[Bsi05/3]	Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 1.0“, Dezember 2005, http://www.bsi.bund.de/literat/bsi_standard/index.htm
[Bsi05/4]	Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.0“, September 2005, http://www.bsi.bund.de/literat/bsi_standard/index.htm
[BsiPol05]	Bundesamt für Sicherheit in der Informationstechnik, „*IT-Sicherheit im KRITIS-Unternehmen - Ein Beispiel aus der Praxis* -“, 2005, http://www.bsi.de/fachthem/kritis/praxisbeispiel.htm
[Cert97]	CERT Coordination Center, „*Security of the Internet*”, 1997, http://www.cert.org/encyc_article/tocencyc.html
[Dan03]	Dancho Danchev, „*Building and Implementing a Successful Information Security Policy*”, 2003, http://www.secinf.net/policy_and_standards/Building_Implementing_Security_Policy1228.html
[Dem05]	Deming in Deutschland, “Die 14 Deming Punkte”, http://www.deming.de/deming/deming3.html, 2005
[EURO95]	Richtlinie 95/46/EG des Europäischen Parlaments, „*Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 – 0050*“, 24. Okober 1995, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML
[Fail99]	Control Data, White Paper „Why Security Policies Fail”, http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf, 1999

[HFBK03]	Harman, B.; Flinn, D.; Beznosov; K.; Kawamoto, S., „*Mastering Web Services Security*“ John Wiley Sons, Inc., New York, 2003
[Hopp03]	Hoppe, Gabriela, “*Sicherheit von Informationssystemen: Gefahren, Maßnahmen und Management im IT-Bereich*“, Verl. Neue Wirtschafts-Briefe, Berlin, 2003
[InfW04]	InformationWeek, „*IT Security Studie 2004”*, April bis Juni 2004, http://www.iw-live.de/security/media/it_security_2004_%20praesentation_ergebnisauszug.pdf
[Init01]	Initiative D21, „IT-Sicherheitskriterien im Vergleich“, Ein Leitfaden der Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung, 2001
[Kes04]	Kes Online/Microsoft, „<kes>/Microsoft-Sicherheitsstudie 2004, Lagebericht zur Informationssicherheit“, 2004, http://www.kes.info/archiv/material/studie2004/index.html
[Mak03/2]	MakoSi-Vorgehensmodell, „*Vorgehensmodell zur Realisierung sicherer Domänen-übergreifender Zusammenarbeit*“, Fachgebiet Datenverarbeitung in der Konstruktion, TU Darmstadt, 6.11.2003
[Kyas02]	Kyas, Othmar, „*IT-Crackdown: Sicherheit im Internet*“, mitp, Bonn, 2002
[Nist95]	National Institute of Standards and Technology, U.S. Department of Commerce, „*An Introduction to Computer Security: The NIST Handbook*”, 1995, http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html
[Opp97]	Opplinger, Rolf, „*IT-Sicherheit: Grundlagen und Umsetzung in der Praxis*“, Vieweg, Braunschweig, 1997
[Pohl04]	Norbert Pohlmann, „*Wirtschaftslichkeitsbetrachtungen von IT-Sicherheitssystemen*“, Fachhochschule Gelsenkirchen 2004, http://www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/Wirtschaftlichkeit_ITsec_06_03_04.pdf
[Ris05]	Rechtsinformationssystem des Bundes (RIS), http://ris.bka.gv.at/
[Sans05]	SANS Institute, „*SANS Security Policy Project*”, 2005, http://www.sans.org/resources/policies/
[Schn00]	Schneier, B., „*Secrets & Lies – IT Sicherheit in einer vernetzten Welt*“, dpunkt.verlag, Heidelberg, 2004
[Sec01]	Charl Van Der Walt, „*Introduction to Security Policies, Part One: An Overview of Policies*“, 2001, http://www.securityfocus.com/infocus/1193
[SecM06]	Securitymanager.de, Umfrage “Handelt und arbeitet Ihr Unternehmen nach einer vorgegebenen IT-Security-Policy?“, http://www.securitymanager.de/community/
[Shir00]	Shirey, R. „*Internet Security Glossary, RFC 2828*“ The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2828.txt, 2000

[Sihb04]	Bundeskanzleramt, IT-Koordination, „*Österreichisches IT-Sicherheitshandbuch*“, Version 2.2 2004, http://www.cio.gv.at/securenetworks/sihb/
[Sihb04/2]	Bundeskanzleramt, IT-Koordination, „*Österreichisches IT-Sicherheitshandbuch*“, Version 2.2 2004, S. 11
[Stro03]	Strobel, Stefan, „*Firewalls und IT-Sicherheit: Grundlagen und Praxis sicherer Netze*“, dpunkt-Verl., Heidelberg, 2003
[Sym04]	Symantec, „*Internet Security Threat Report*“, 2004, http://www.symantec.com/region/de/PressCenter/Threat_Reports.html
[Wiki01]	Wikipedia, 2005, „*Ziel*”, http://de.wikipedia.org/wiki/Ziel
[Wiki02]	Wikipedia, 2005, „*Kriterium*”, http://de.wikipedia.org/wiki/Kriterium

11 Anhang

11.1 Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplom- bzw. Magisterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Des weiteren versichere ich, dass ich diese Diplom- bzw. Magisterarbeit weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Linz, am 13. November 2006 …….

Stefan Klement

11.2 Curriculum Vitae

Stefan Christian Klement

* 1975 in Salzburg

Anschrift:
Herrenstr. 41
4020 Linz
Telefon: +43 699/ 18005031
e-mail: stefan.klement@gmx.net

Familienstand:
ledig; keine Kinder

Nationalität:
Österreich

Ausbildung

1981 - 1985	Volksschule in Salzburg/Elixhausen
1985 - 1989	Unterstufe des Bundesgymnasium Christian-Doppler in Salzburg
1989 - 1994	HTL für Elektronik/Informatik, Ausbildungszweig Nachrichtentechnik
Okt. 1994 – Juni 1995	Präsenzdienst in Salzburg/Siezenheim, Schwarzenbergkaserne
seit Okt. 1995	Studium der Wirtschaftsinformatik an der Johannes Kepler Universität Linz
Dez. 2005 – Feb. 2006	Projektmanagement Lehrgang: Grundlagen und Prozesse des Projektmanagement
März 2006	pma - Zertifizierung als Projektmanager (IPMA-Level C)

Berufserfahrung

Juli – Sept. 1995	Sony DADC Austria AG – CD Erzeugung, Anif Betreuung der Netzwerkinfrastruktur
1997-1999	Schulungstätigkeiten am WiFi Linz Betreuung von IT-Infrastruktur mehrerer Unternehmen, Linz
seit Juni 2000	Ebit GmbH - Hersteller von CRM Standardsoftware für Call und Customer Care Center, Linz Tätigkeit im Projektmanagement, IT–Services, Konzeption und Betreuung IT-Infrastruktur, Sicherheits- und Notfallkonzepte

Zusätzliches

Sprachkenntnisse**:**
Englisch

Führerschein**:**
Gruppe B

Linz, am 13. November 2006