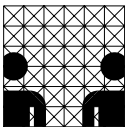
Universität Hamburg

Fachbereich Informatik



Diplomarbeit:

Möglichkeiten und Auswirkungen der Integration der Nutzer in die Erstellung und Durchsetzung einer IT-Sicherheitspolitik

Michael Krooß

Betreuung:

Prof. Dr. Klaus Brunnstein
Dr. Hans-Joachim Mück

5. Februar 2003

Dank sagen möchte ich meinen Betreuern Herrn Prof. Dr. Klaus Brunnstein und Herrn Dr. Hans-Joachim Mück, die mich während der gesamten Erstellung der Arbeit unterstützt haben. Ferner möchte ich Herrn Arslan Brömme danken, der mir in der Phase der Themenfindung geholfen hat, aus einer groben Vorstellung ein ausgearbeitetes Konzept zu entwickeln. Schließlich möchte ich mich bei Frau Martina Timmann und Herrn Markus Lange bedanken, die die undankbare Aufgabe auf sich genommen haben, die fast fertige Arbeit nach Fehlern und Schwächen durchzusehen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACM	Association for Computing Machinery
ATM	Asynchronous Transfer Mode
ATMARP	Asynchronous Transfer Mode Address Resolution Protocol
BSI	Bundesamt für die Sicherheit in der Informationstechnik
DFN	Deutsches Forschungsnetz
DV	Datenverarbeitung
FAQ	Frequently Asked Questions
GoB	Grundsätze ordnungsmäßiger Buchführung
HGB	Handelsgesetzbuch
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IFIP	International Federation for Information Processing
IP	Internet Protocol
IRS	Intrusion Response System
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
OSI	Open System Interconnection
PIN	Persönliche Identifikationsnummer
RFC	Request for Comment
SO	Subjekt-Objekt(-Beziehungen)
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
UDP	User Datagram Protocol
VBS	Visual Basic Script
VPN	Virtual Private Network

Kapitel 1

Einleitung

In diesem Kapitel soll im Abschnitt 1.1 zunächst das Thema dieser Diplomarbeit motiviert und im darauf folgenden Abschnitt 1.2 die Zielsetzung bestimmt werden. Danach soll im Abschnitt 1.3 die zur Erreichung der Zielsetzung verwendete Vorgehensweise erläutert und im Abschnitt 1.4 der Aufbau dieser Arbeit aufgezeigt werden.

1.1 Motivation

In diesem Abschnitt soll zu Anfang die grundsätzliche Unsicherheit, die beim Einsatz von IT-Systemen besteht, ausgeführt werden. Anschließend soll aufgezeigt werden, mit welchen Maßnahmen dieser Unsicherheit bisher begegnet wurde. Abschließend soll begründet werden, warum diese Maßnahmen nicht ausreichend sind.

Der Einsatz von Informationstechnik (IT) leidet grundsätzlich unter einer großen Unsicherheit, die sich aus der Anfälligkeit der eingesetzten Systeme gegenüber vielen verschiedenartigen Bedrohungen (höhere Gewalt, Angriffe, Bedienungsfehler, etc.) ergibt. Diese Anfälligkeit liegt den IT-Systemen oft inhärent zugrunde. Sie hat ihre Ursachen also nicht nur in Fehlern in der Anwendung, dem Einsatz und der Implementierung, sondern kann insbesondere auch auf Fehler in der Spezifikation und dem Design zurückgeführt werden (vgl. [Bru93, Seite 78ff.]). Seit dem Aufkommen der IT-Systeme wurde auf verschiedene Arten versucht dieser Anfälligkeit entgegenzuwirken.

Zunächst wurden IT-Systeme hauptsächlich in militärischen und wissenschaftlichen Bereichen genutzt. Die Personen, die die IT-Systeme nutzten, waren in der Regel auch deren Administratoren. Der Schutz der IT-Systeme bestand vorwiegend aus physikalischen und organisatorischen Maßnahmen. Die IT-Systeme wurden zentral in geschlossenen Räumen betrieben, zu denen nur berechtigten Personen Zutritt gewährt wurde. Unter Umständen gab es zusätzlich abschließbare Metallschränke, in denen die Nutzer ihre Datenträger lagern konnten, um ihre Daten vor Bedrohungen wie dem unberechtigten Zugriff durch andere Nutzer zu schützen (vgl. [Hig93, Seite 2]).

Später erfolgte eine zunehmende Dezentralisierung der IT-Systeme. Diese Entwicklung hatte zur Folge, dass sowohl die Anzahl der Personen, die direkt mit IT-Systemen in Berüh-

rung kamen, als auch die Masse und der Schutzbedarf der auf IT-Systemen verarbeiteten und gelagerten Daten immens stieg. Auf der einen Seite vergrößerte sich die Abhängigkeit von der Verfügbarkeit und der Korrektheit der Daten, auf der anderen Seite wurde es vor allem durch die steigende Komplexität der IT-Systeme immer schwieriger, die Plausibilität der Ergebnisse ihrer Verarbeitung zu überprüfen (vgl. [Bru93, Seite 81]). Da die bisherigen Maßnahmen nicht mehr angemessen waren, wurden vermehrt technische Maßnahmen eingeführt. Dabei wurden die Personen, die mit den IT-Systemen arbeiteten, oft als eine Schwachstelle oder sogar als eine Bedrohung gesehen, deren „Unzulänglichkeiten“ mit dem Einsatz von technischen Maßnahmen ausgeglichen werden sollten.

Viele dieser Maßnahmen werden auch heute noch eingesetzt: Dabei werden oft nicht mehr die Zutrittsmöglichkeiten zu den Räumen, sondern die Zugänge eines IT-Systems durch Identifikation und Authentisierung der Personen gegenüber dem IT-System kontrolliert. Der Zugriff auf Daten wird nicht mehr durch Metallschränke, sondern durch Zugriffsrechte beschränkt, die vom IT-System durchzusetzen sind. Die zunehmende Vernetzung führte zum Einsatz von „Firewalls“, „Intrusion Detection Systems“ (IDS), kryptographischer Verfahren, aber auch zum verstärkten Einsatz von „Antimalware“-Software. Dabei ist zu beachten, dass viele dieser Schutzmechanismen nicht nur Unsicherheiten einschränken, sondern auch neue Probleme schaffen können, denen in der Folge auf andere Weise begegnet werden muss.

Es wurden verschiedene Kriterienkataloge aufgestellt, deren Ziel es ist, einen Maßstab zur Bewertung der Sicherheit von IT-Systemen zu bieten (vgl. [BFH92, Seite 393f.]). Beispiele hierfür sind die „Trusted Computer System Evaluation Criteria“ (TCSEC) des „Department of Defense“ der USA, die aufgrund der Farbe des Einbands oft als “Orange Book“ bezeichnet werden (vgl. [DoD85]), die „Information Technology Security Evaluation Criteria“ (ITSEC), die u.a. von Frankreich, Großbritannien und Deutschland entwickelt wurden (vgl. [ITS91]), und die „Common Criteria“, die eine Harmonisierung zwischen den Kriterienkatalogen der USA, Kanada und aus Europa darstellen (vgl. [CC999]).

Es zeigt sich aber, dass der Einsatz von IT-Systemen trotz dieser Ansätze immer noch mit einer großen Unsicherheit behaftet ist. Diese Unsicherheit ist insbesondere in Bereichen als sehr problematisch anzusehen, in denen kritische Prozesse durch IT-Systeme unterstützt oder sogar gesteuert werden bzw. die Existenz einer Organisation von dem Einsatz der IT-Systeme abhängt.

Langfristig wird es notwendig sein, „beherrschbare“ Systeme zu entwickeln, die „die angeborenen Schwächen heutiger Systeme nachweisbar ausschließen müssen“ (vgl. [Bru02]). Solange derartige Systeme noch nicht existieren, wird es weiterhin notwendig sein, den durch die Anfälligkeit der IT-Systeme bedingten Risiken, die nicht in einem akzeptablen Rahmen liegen, mit Schutzmaßnahmen zu begegnen. Das mit dem Einsatz von Schutzmaßnahmen verfolgte Ziel ist, die bestehenden Risiken soweit zu verringern, dass das verbleibende Restrisiko ein akzeptables Niveau erreicht.

Hier soll der Standpunkt vertreten werden, dass es nicht immer möglich bzw. angemessen ist, dieses Ziel ausschließlich mit technischen oder physikalischen Schutzmaßnahmen zu erreichen. Stattdessen sollte der „menschlichen Seite des Sicherheitsmanagements“ mehr Aufmerksamkeit geschenkt werden (vgl. [Hig93, Seite 8f.]).

1.2 Zielsetzung der Arbeit

Im Rahmen dieser Diplomarbeit soll betrachtet werden, wie sich die Einbeziehung der Nutzer bei der Festlegung und Durchführung von Maßnahmen zur Verringerung der Anfälligkeiten von IT-Systemen auf die Sicherheit der IT-Systeme auswirken kann. Da Maßnahmen zur Erhöhung der Sicherheit von IT-Systemen oft in so genannten IT-Sicherheitspolitiken (IT Security Policies) festgeschrieben werden, soll dabei eine Orientierung an der Erstellung und Durchsetzung einer Sicherheitspolitik für IT-Systeme erfolgen. Es sollen beispielhaft einige Maßnahmen zur Vorbeugung vor und Erkennung von sicherheitsrelevanten Ereignissen aufgezeigt werden, bei denen eine Einbeziehung der Nutzer erfolgt. Diese sollen im Hinblick auf ihre Vor- und Nachteile auch im Verhältnis zu herkömmlichen Maßnahmen betrachtet werden. Dabei soll insbesondere eine Betrachtung der positiven und negativen Auswirkungen der Einbeziehung der Nutzer für die Organisation und die Nutzer erfolgen.

1.3 Vorgehen

Zunächst soll eine Einführung und Abgrenzung der in dieser Arbeit verwendeten Begriffe und Sachverhalte erfolgen. Danach soll näher betrachtet werden, wie sich verschiedene Grade der Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik auswirken können. Dem soll eine Betrachtung verschiedener Maßnahmen folgen, bei denen die Nutzer bei der Vorbeugung und Erkennung von sicherheitsrelevanten Vorfällen einbezogen werden. Dazu soll zunächst eine Menge von Szenarien aufgestellt werden, in denen eine Darstellung von denkbaren Vorfällen erfolgt. Dabei soll insbesondere eine Berücksichtigung der verschiedenen Rollen, in denen die Nutzer auftreten können, durchgeführt werden (z.B. Nutzer ist selbst Angreifer, Nutzer ist Schwachstelle). Dann sollen verschiedene Schutzmaßnahmen aufgezeigt werden, bei denen eine aktive Einbeziehung der Nutzer erfolgt. Diese sollen zunächst im Hinblick auf ihre Eignung und zu erwartende Wirksamkeit betrachtet und anschließend diesbezüglich mit herkömmlichen Maßnahmen verglichen werden. Abschließend soll eine Betrachtung der Möglichkeiten zur Durchsetzung der Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, durchgeführt werden.

1.4 Aufbau der Arbeit

Die Einführung und Abgrenzung der in dieser Arbeit verwendeten Begriffe und Sachverhalte soll im Kapitel 2 erfolgen. Die Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik soll in Kapitel 3 betrachtet werden. Die Aufstellung der Szenarien soll in Kapitel 4, die Aufstellung der Schutzmaßnahmen in Kapitel 5 erfolgen. Die Betrachtung der Wirksamkeit dieser Maßnahmen soll im Kapitel 6, der Vergleich mit herkömmlichen Maßnahmen im Kapitel 7 durchgeführt werden. Die Betrachtung der Möglichkeiten der Durchsetzung soll im Kapitel 8 erfolgen. Abschließend erfolgt im Kapitel 9 eine Zusammenfassung der Ergebnisse und ein Ausblick auf Fragestellungen, die sich im Rahmen der Erstellung dieser Arbeit ergeben haben.

Kapitel 2

Einführung und Abgrenzung von verwendeten Begriffen

- Ziel:
  Einführung von Begriffen und Sachverhalten, die in dieser Arbeit kapitelübergreifend verwendet werden.
- Vorgehen:
  1. Einführung „Sicherheit von IT-Systemen“
  2. Einführung in Aufgabe und Erstellung von IT-Sicherheitspolitiken
  3. Abgrenzung von Personengruppen wie Nutzer, Administratoren, etc.

In diesem Kapitel soll eine Einführung der Begriffe und Sachverhalte erfolgen, die in dieser Arbeit kapitelübergreifend verwendet werden. Begonnen wird dabei im Abschnitt 2.1 mit einer Bestimmung des Begriffs Informationstechnik-System (IT-System) und einer Einführung in Begriffe aus dem Bereich der Sicherheit und des Schutzes von IT-Systemen. Anschließend folgt im Abschnitt 2.2 eine Einführung in das Thema der IT-Sicherheitspolitiken. Neben einer Begriffsbestimmung sollen dabei mögliche Formen und Inhalte von IT-Sicherheitspolitiken aufgezeigt werden. Ferner werden die Phasen der Erstellung einer IT-Sicherheitspolitik diskutiert. Dann schließt sich im Abschnitt 2.3 eine Bestimmung des Begriffs Nutzer und eine Abgrenzung von diesem zu Begriffen wie Administrator und Management an. Abschließend wird im Abschnitt 2.4 eine Zusammenfassung dieses Kapitels erfolgen.

2.1 Einführung in die Sicherheit von IT-Systemen

In diesem Abschnitt soll zunächst im Unterabschnitt 2.1.1 eine Bestimmung des Begriffs IT-System erfolgen. Dann sollen im Unterabschnitt 2.1.2 die beim Betrieb von IT-Systemen bestehenden Unsicherheiten und im Unterabschnitt 2.1.3 Möglichkeiten des Schutzes von IT-Systemen betrachtet werden.

2.1.1 Begriffsbestimmung IT-System

Werden Informationen in irgendeiner Form dargestellt, so spricht man oft von informationstragenden Daten oder einfach **Daten**. Die Darstellung von Informationen als Daten ist im Allgemeinen abhängig von einem Kontext, z.B. von der Art der Codierung von Zeichen oder der dabei verwendeten Sprache. Die Darstellung von Informationen als Daten geschieht oft zur Aufbewahrung, Übertragung oder Verarbeitung der Informationen.

Unter einem **Informationstechnik-System (IT-System)** oder auch **Datenverarbeitungssystem** soll in dieser Arbeit ein System zur Aufbewahrung, Übertragung oder Verarbeitung von informationstragenden Daten verstanden werden (vgl. [Opp97, Seite 3]). Ein IT-System umfasst eine Ansammlung von Hardware (insbesondere auch Datenträger), Software und Daten sowie die Personen, die berechtigt sind, auf diese Ansammlung oder Teile dieser Ansammlung zuzugreifen (vgl. [Pfl96, Seite 3]).

2.1.2 Unsicherheit von IT-Systemen

IT-Systeme haben im Allgemeinen **Schwachstellen** bzw. **Verwundbarkeiten** (Vulnerabilities). Diese Schwachstellen können ihre Ursachen z.B. in einer nicht angemessenen Spezifikation, einer fehlerhaften Implementierung oder in der Art und Weise des Einsatzes eines IT-Systems haben. Ferner ergeben sich aus der Umgebung **Bedrohungen** (Threats), denen IT-Systeme oder Teile von IT-Systemen ausgesetzt sind. Das „Bundesamt für die Sicherheit in der Informationstechnik“ (BSI) führt in dem von ihm veröffentlichten IT-Grundschutzhandbuch eine Einteilung von Bedrohungen in fünf Kataloge durch (vgl. [BSI01, Gefährdungskataloge]). Dabei ist es nicht immer möglich, jede Bedrohung eindeutig einem der im Folgenden aufgeführten Kataloge zuzuordnen.

1. **Höhere Gewalt**
   Hierzu werden z.B. Bedrohungen durch Blitz, Feuer oder Sturm gezählt.

2. **Organisatorische Mängel**
   Hierzu zählen z.B. fehlende oder auch unzureichende Regelungen und unzureichende Kenntnis über Regelungen.

3. **Menschliche Fehlhandlungen**
   Hierzu werden z.B. Fahrlässigkeit und Nichtbeachtung von Regelungen gezählt.

4. **Technische Mängel**
   Hierzu werden z.B. Ausfall und Fehler der Hard- und Software gezählt.

5. **Vorsätzliche Handlungen**
   Bei vorsätzlichen Handlungen werden Bedrohungen von Personen bewusst herbeigeführt. Im Folgenden wird in diesem Zusammenhang von **Angriffen** bzw. **Angreifern** gesprochen werden (vgl. Abschnitt 2.3).

Als **Risiko** wird die Möglichkeit bezeichnet, einen **Schaden** zu erleiden. Risiken ergeben sich dadurch, dass eine Bedrohung auf eine Verwundbarkeit treffen kann (vgl. [Opp97, Seite 5f.]).

2.1.3 Schutz von IT-Systemen

Um die Risiken, denen ein IT-System ausgesetzt ist, zu verringern, können **Schutzmaßnahmen** eingesetzt werden. Schutzmaßnahmen verringern die Risiken, indem sie die Verwundbarkeit eines IT-Systems verringern (vgl. [Pfl96, Seite 3]). Unter **Restrisiko** versteht man das trotz des Einsatzes von Schutzmaßnahmen verbleibende Risiko. Schutzmaßnahmen können unterschieden werden in (vgl. [Opp97, Seite 6]):

- physikalisch (z.B. bauliche Schutzvorkehrungen)
- organisatorisch (z.B. administrative und personelle Maßnahmen)
- technisch (z.B. Verschlüsselung, Signierung)

Ihre Wirkung kann unterschieden werden in (vgl. [Opp97, Seite 6]):

- präventiv (vorbeugende Maßnahmen)
- detektiv (erkennende Maßnahmen)
- korrektiv (wiederherstellende Maßnahmen)

Schutzmaßnahmen wirken im Allgemeinen nicht nur gegen eine, sondern oft gegen mehrere Verwundbarkeiten. Werden mehrere Schutzmaßnahmen eingesetzt, so kann unterschieden werden, ob ihre Wirkungen komplementär (sich ergänzend), konkurrierend (sich beeinträchtigend) oder orthogonal (es bestehen keine Wechselwirkungen) zueinander sind.

Bei der Art der Auswahl von Schutzmaßnahmen kann grob zwischen **Grundschutz** und **individuellem Schutz** (custom tailored) unterschieden werden.

- Beim Grundschutz wird der Ansatz verfolgt, durch die pauschale Auswahl geeigneter Sicherheitsmechanismen eine Absicherung gegen die gängigsten Risiken zu erreichen (vgl. [Ned99, Seite 11]).
- Beim individuellen Schutz werden in einer detaillierten **Risikoanalyse** (Risk Analysis) die Teile eines IT-Systems identifiziert, die **schutzbedürftige Werte** (Assets) darstellen, und deren **Schutzbedarf** ermittelt. Anhand dieser Informationen können dann angemessene Schutzmaßnahmen ausgewählt werden. Auf die hier angedeutete Vorgehensweise wird noch detaillierter im Rahmen des Unterabschnitts 2.2.4 eingegangen werden.

Ein großer Vorteil beim Ansatz des Grundschutzes ist, dass grundsätzlich keine Ressourcen für eine detaillierte Risikoanalyse aufgewendet werden müssen (vgl. [Ned99, Seite 11]). Als Nachteil muss aber gesehen werden, dass es bei einzelnen Werten mit hohem Schutzbedarf denkbar ist, dass dieser durch die pauschale Einstufung unter Umständen nicht angemessen berücksichtigt wird.

Die durch den Einsatz von Schutzmaßnahmen verfolgten **Schutzziele** werden oft in die folgenden drei Klassen aufgeteilt:

- Wahrung der **Vertraulichkeit**
  Man spricht von Vertraulichkeit, wenn ausschließlich eine autorisierte Kenntnisnahme stattfindet. Besondere Bedeutung hat die Vertraulichkeit von Daten.

- Wahrung der **Integrität**
  Man spricht von Integrität, wenn ausschließlich autorisierte Modifikation stattfindet. Neben der Integrität der Daten hat auch die Integrität der Software und Hardware eine besondere Bedeutung.

- Wahrung der **Verfügbarkeit**
  Man spricht von Verfügbarkeit, wenn die Nutzung für autorisierte Zwecke möglich ist. Die Verfügbarkeit eines IT-Systems oder von Teilen eines IT-Systems kann außer durch andere Bedrohungen auch durch eine autorisierte Nutzung eingeschränkt oder im Extremfall unterbunden werden. Als Beispiel sei die Verfügbarkeit von begrenzten Ressourcen wie z.B. Rechenzeit auf einem Server oder ein von mehreren Nutzern verwendeter Drucker genannt (diese Möglichkeit wird im Unterabschnitt 4.3.4 aufgegriffen werden). Die Verfügbarkeit hat im Allgemeinen für alle Teile eines IT-Systems eine hohe Bedeutung.

Eine vierte Klasse, die gerade in jüngster Zeit bei steigender Verteilung und kommerzieller Nutzung von IT-Systemen an Bedeutung gewonnen hat, ist die **Verbindlichkeit** oder **Nicht-Abstreitbarkeit**. Ziel bei der Nicht-Abstreitbarkeit ist es, eine Nachweisbarkeit von Handlungen zu gewährleisten. Dies ist z.B. bei der Verbindlichkeit von Rechtsgeschäften und der Abrechnung von kommerziellen Diensten von Interesse. Im Allgemeinen wird aber die Ansicht vertreten, dass diese Klasse nicht „orthogonal“ zu den bereits genannten Klassen ist. Das bedeutet insbesondere, dass zur Realisierung von Nicht-Abstreitbarkeit Mechanismen aus den oben genannten Klassen verwendet werden können (vgl. [Gel00, Seite 7]).

Bei der Aufzählung der Schutzklassen wurde mehrfach von autorisierten Handlungen ausgegangen. Welche Handlungen autorisiert sind, ist gerade bei großen und komplexen IT-Systemen nicht immer intuitiv zu entscheiden. Daher ist es im Allgemeinen notwendig, Regelungen zu finden, nach denen entschieden werden kann, welche Handlungen als autorisiert anzusehen sind. Dies geschieht oft im Rahmen einer **IT-Sicherheitsstrategie** oder auch **IT-Sicherheitspolitik** (IT Security Policy).

2.2 Einführung in IT-Sicherheitspolitiken

In diesem Abschnitt soll zunächst eine Bestimmung des Begriffs IT-Sicherheitspolitik erfolgen (vgl. Unterabschnitt 2.2.1). Dann soll aufgezeigt werden, in welcher Form IT-Sicherheitspolitiken vorliegen können (vgl. Unterabschnitt 2.2.2). Im Anschluss soll aufgezeigt werden, welche Inhalte in IT-Sicherheitspolitiken aufgeführt sein können (vgl. Unterabschnitt 2.2.3) und ein exemplarisches Vorgehensmodell für die Erstellung von IT-Sicherheitspolitiken diskutiert werden (vgl. Unterabschnitt 2.2.4).

2.2.1 Begriffsbestimmung IT-Sicherheitspolitik

Für den Begriff „IT-Sicherheitspolitik“ gibt es in der Literatur kein einheitliches Verständnis. So stellt Sterne (vgl. [Ste91, Seite 221]) fest, dass der Begriff im so genannten „Orange Book“ (vgl. [DoD85, Seite 2 bzw. Seite 112]) und an anderer Stelle unter anderen in den folgenden beiden Weisen verwendet wird:

1. in Bezug auf Regeln, die Handlungen von menschlichen Subjekten (Personen) betreffen,

2. in Bezug auf Regeln, die Handlungen (Zugriffe) von automatischen Subjekten (z.B. Prozesse auf einem IT-System) betreffen.

Eine IT-Sicherheitspolitik im Sinne des Falles 2 findet sich zum Beispiel in [Hol02]. Dort wird ein so genanntes „Policy-Modul“ für einen Server zur Auflösung von IP- (Internet Protokoll) nach ATM-Adressen (Asynchronous Transfer Mode Address Resolution Protocol Server, ATMARP-Server) beschrieben, das aufgrund von vorgegebenen Regeln entscheidet, ob eine Anfrage legitim ist, und daher vom Server mit der angefragten Adresszuordnung beantwortet werden soll. Diese Arten von IT-Sicherheitspolitiken sollen im Rahmen dieser Arbeit nicht weiter betrachtet werden. Stattdessen soll hier auf IT-Sicherheitspolitiken im Sinne des Falles 1 eingegangen werden. Eine solche IT-Sicherheitspolitik soll festlegen, welche Regeln hinsichtlich der Sicherheit von IT-Systemen gelten. In einem weiteren Sinne können in einer IT-Sicherheitspolitik auch die zur Durchsetzung durchzuführenden Maßnahmen festgelegt sein. Dabei sollte angestrebt werden, dass dem Einsatz der Maßnahmen ein durchdachtes Gesamtkonzept zugrunde liegt. Als Gegenbeispiel hierzu sei ein Flickwerk aus Maßnahmen genannt, die als Reaktion auf konkrete Vorfälle oder Warnungen in der Presse installiert wurden.

Ølnes stellt fest (vgl. [Øln94, Seite 628]), dass es für die IT-Sicherheitspolitik eines Unternehmens keine „vordefinierte Antwort“ gibt. Ølnes führt dies auf Unterschiede im Sicherheitsbedarf und in der Organisation, Kultur und Arbeitsweise bei verschiedenen Unternehmen zurück.

Um einer unnötigen Beschränkung der Allgemeinheit entgegenzuwirken, sollen in dieser Arbeit grundsätzlich nicht nur Unternehmen, wie z.B. international tätige Konzerne, Aktiengesellschaften usw., sondern auch andere IT-Systeme betreibende Einrichtungen, wie z.B. Behörden, Universitäten oder militärische Einrichtungen, betrachtet werden. Daher soll im Folgenden allgemein von Organisationen ausgegangen werden.

2.2.2 Formen von IT-Sicherheitspolitiken

IT-Sicherheitspolitiken können abhängig vom Sicherheitsbedarf und der Größe des Geltungsbereichs unterschiedliche Formen haben. Sie können implizit oder explizit definiert sein. Implizite IT-Sicherheitspolitiken können zum Beispiel in Form von implementierten Sicherheitsmechanismen oder auch ausschließlich im Bewusstsein des Verantwortlichen existieren. Explizite IT-Sicherheitspolitiken können zum Beispiel aus einem einzelnen Dokument, aus einer Reihe zusammengehörender Dokumente oder auch nur aus einem „Slogan“ bestehen. Wird eine IT-Sicherheitspolitik in mehrere Dokumente aufgeteilt, kann dies nach Themen (zum Beispiel für Nutzer, Netzwerke, Backup, etc.) oder nach dem Grad der Detaillierung (generelle Ziele, konkrete Maßnahmen, konkrete Aspekte der Durchsetzung und Implementierung) geschehen (vgl. [Gro99, Seite 57ff.]).

2.2.3 Inhalt von IT-Sicherheitspolitiken

In diesem Unterabschnitt sollen einige Punkte aufgezählt werden, die in IT-Sicherheitspolitiken aufgeführt sein können. Wie bereits angedeutet, gibt es hier aber keine allgemein gültigen Regeln darüber, ob und in welchem Maße diese oder andere Punkte in einer IT-Sicherheitspolitik aufgeführt sein sollten.

Festlegung des Geltungsbereichs

Eine IT-Sicherheitspolitik sollte festlegen, welchen Geltungsbereich sie umfasst. Dies ist insbesondere dann wichtig, wenn dieser intuitiv nicht eindeutig zu bestimmen ist. Dieser Fall kann zum Beispiel in einer großen Organisation auftreten, in der für einzelne Einheiten aufgrund unterschiedlicher Sicherheitsbedarfe verschiedene IT-Sicherheitspolitiken gelten. Man spricht in diesem Fall von unterschiedlichen Sicherheitszonen.

Festlegung der Ziele

In einer IT-Sicherheitspolitik sollte der zu erzielende Grad an Schutz definiert werden. Dies kann für den gesamten Geltungsbereich allgemein, aber auch für einzelne, vielleicht besonders zu schützende Werte geschehen.

Festlegung von zugelassenen bzw. nicht zugelassenen Handlungen

Es sollte festgelegt werden, vor welchen Ereignissen geschützt werden soll bzw. welche Handlungen zugelassen sein sollen. Dies gilt insbesondere auch für Handlungen von autorisierten Nutzern. So kann es z.B. wichtig sein, explizit zu klären, ob und unter welchen Umständen Ressourcen für private Zwecke genutzt werden dürfen.

Grundsätzlich können entweder alle Handlungen aufgezählt werden, die verboten sind (Verbotsregeln), oder alle Handlungen, die erlaubt sind (Erlaubnisregeln). Dabei gilt allgemein, dass bei der Aufstellung von Verbotsregeln die Gefahr besteht, relevante Regeln

zu übersehen, und dass die Aufstellung von Erlaubnisregeln oft sehr aufwendig und unübersichtlich werden kann. Ferner sollte explizit festgehalten werden, dass Regelungen von niemanden umgangen werden dürfen (bzw. die Ausnahmefälle aufgeführt werden, in denen die Umgehung legitim ist). Dies kann notwendig sein, um ein Bewusstsein für die Verbindlichkeit, der durch die IT-Sicherheitspolitik durchzusetzenden Maßnahmen, zu erzeugen.

Festlegung von Maßnahmen

Es sollte festgehalten werden, ob der zu erzielende Schutz durch Grundschutz oder durch einen individuellen Schutz erreicht werden soll (vgl. Unterabschnitt 2.1.3). Es sollten entsprechende Maßnahmen definiert werden.

Durchsetzung der IT-Sicherheitspolitik

Innerhalb einer IT-Sicherheitspolitik sollte festgelegt werden, wie die Durchsetzung der Maßnahmen erfolgen soll. Hierbei sind zum Beispiel Verantwortliche zu nennen, die für die Durchsetzung und die Überprüfung einzelner Teile zuständig sind. Es sollten Maßnahmen (Sanktionen) aufgeführt werden, die bei Verstößen gegen die IT-Sicherheitspolitik durchzuführen sind.

Vorfallsbehandlung

Ferner sollten Verfahren festgelegt werden, die das Vorgehen bei einem eingetretenen Vorfall regeln. Hierbei sind zum Beispiel Verantwortliche festzulegen, die benachrichtigt werden müssen (vgl. [Øln94, Seite 635]). Aber auch konkrete Maßnahmen sollten festgeschrieben werden (vgl. [Gro99, Seite 64f.] und [Fra97]).

Weiterentwicklung der IT-Sicherheitspolitik

Es sollten auch Ereignisse, die eine Überarbeitung der IT-Sicherheitspolitik erfordern, festgeschrieben werden (vgl. [Øln94, Seite 634]). Dies können zum Beispiel eingetretene Vorfälle, die nicht oder nicht im richtigen Maße berücksichtigt wurden, Gesetzesänderungen oder der Weggang von Verantwortlichen sein.

Dokumentation der Erstellung

Damit eine Weiterentwicklung einer IT-Sicherheitspolitik möglich ist, sollte dokumentiert werden, welche Annahmen bei der Erstellung getroffen wurden und welche Begründungen zu durchgesetzten, aber auch zu nicht durchgesetzten Maßnahmen geführt haben (vgl. [Øln94, Seite 634]).

2.2.4 Erstellung einer IT-Sicherheitspolitik

In diesem Unterabschnitt soll ein grobes Vorgehen zur Erstellung einer IT-Sicherheitspolitik skizziert werden (vgl. Abbildung 2.1). Das Ziel bei einem solchen Verfahren sollte sein,

festzustellen was geschützt werden soll, wovor es geschützt werden soll und wie es geschützt werden soll (vgl. [Fra97, Seite 5]). Ein Verfahren, wie es hier dargestellt wird, ist im Allgemeinen nur für große Organisationen durchführbar, da es ein hohes Maß an finanziellen und personellen Ressourcen benötigt.

Aufstellung eines Teams zur Erstellung einer IT-Sicherheitspolitik

Zunächst muss ein für die Erstellung der IT-Sicherheitspolitik verantwortliches Team aufgestellt werden. Bei der Aufstellung ist zu beachten, dass zur Erstellung einer detaillierten IT-Sicherheitspolitik Kenntnisse aus verschiedenen Bereichen notwendig sind. Ferner sollten die Personengruppen einbezogen werden, ohne deren Unterstützung die erfolgreiche Durchsetzung der IT-Sicherheitspolitik gefährdet wäre. Im Folgenden sollen angelehnt an [Gro99, Seite 61] einige einzubeziehende Personengruppen aufgezählt und jeweils Begründungen für eine Einbeziehung gegeben werden.

- verantwortliches Management:
  Die Durchsetzung einer IT-Sicherheitspolitik erfordert die Unterstützung des Managements. Dies gilt sowohl für die Einführung von in der IT-Sicherheitspolitik festgelegten Maßnahmen als auch für eine Vorbildrolle bei ihrer Einhaltung und für die eventuell notwendige Durchführung von Sanktionen bei Verstößen.

- betroffene Mitarbeiter:
  Im Allgemeinen haben Mitarbeiter den besten Einblick in bestehende Arbeitsabläufe, Vorgehensweisen und den damit verbundenen Problemen. Ferner ist ihre Einbeziehung oft notwendig, um einer grundsätzlich ablehnenden Haltung und daraus folgend einer mangelnden Unterstützung für die durchgeführten Maßnahmen entgegenzuwirken (vgl. Kapitel 3).

- Sicherheitsdienst:
  Im Allgemeinen werden bei der Erstellung einer IT-Sicherheitspolitik bereits Sicherheitsmaßnahmen bestehen. Für diese Maßnahmen verantwortliche Mitarbeiter sind oft am Besten in der Lage, diese zu beschreiben und ihre Wirksamkeit zu beurteilen. Ferner haben sie oft bessere Möglichkeiten bei der Einschätzung der Machbarkeit und den Möglichkeiten zur Durchsetzung von neuen Maßnahmen.

- Betriebsrat und -datenschützer:
  Bei verschiedenen Schutzmaßnahmen ist eine Verletzung der (Persönlichkeits-)Rechte der Mitarbeiter möglich. Dies gilt insbesondere für das „Logging“, bei dem Handlungen und Ereignisse für eine Auswertung im Hinblick auf sicherheitskritische Ereignisse aufgezeichnet werden. Derartige Maßnahmen sollten bereits bei der Erstellung der IT-Sicherheitspolitik mit den für diese Fragen verantwortlichen Personen abgesprochen werden.

- Rechtsberater und Datenschützer:
  Es ist sehr wichtig, dass die IT-Sicherheitspolitik mit geltendem Recht verträglich

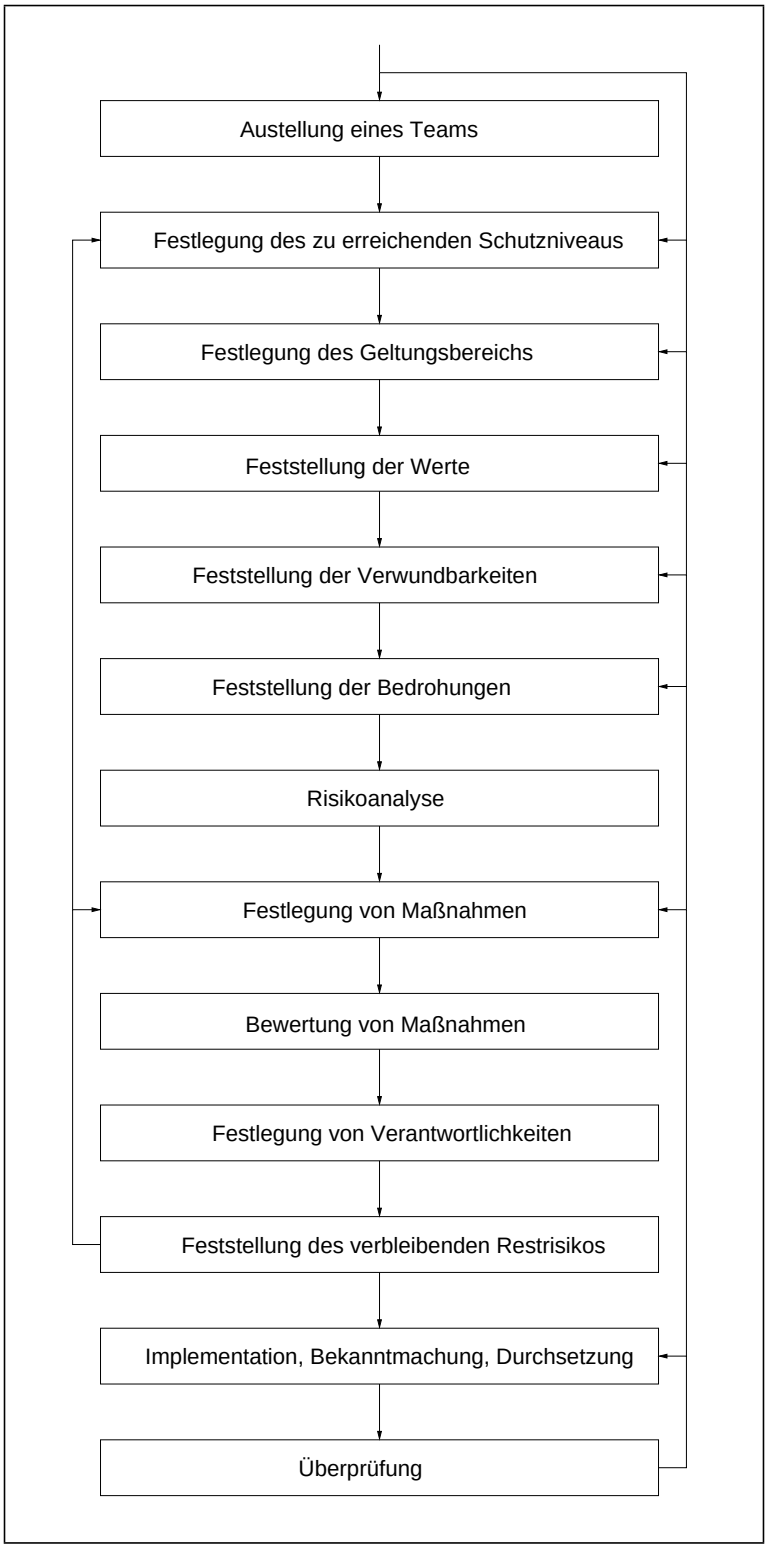


Abbildung 2.1: Phasen der Erstellung einer IT-Sicherheitspolitik

ist. Dies gilt insbesondere im Bereich des Datenschutzes. Ist entsprechende Expertise innerhalb der Organisation nicht verfügbar, sollten externe Experten herangezogen werden (vgl. [Fra97, Seite 10]).

- Versicherungen:
  Versicherungen können über fundiertere Schätzungen über Ausmaß und Wahrscheinlichkeit von Schäden verfügen. Ferner kann es bei einigen Bedrohungen sinnvoll sein, die damit verbundenen Risiken soweit möglich auf eine Versicherung zu übertragen (vgl. [Kos00, Seite 64]).

Festlegung des zu erreichenden Schutzniveaus

Es sollte festgelegt werden, welches Schutzniveau generell zu erreichen ist (vgl. [Øln94, Seite 630]). Ein generelles Schutzniveau ergibt sich einerseits aus dem generellen Schutzbedarf, der bei Banken, Versicherungen oder militärischen Einrichtung im Allgemeinen höher als zum Beispiel bei Bibliotheken oder Universitäten sein wird, und andererseits aus den zur Verfügung stehenden Ressourcen. Generell steigt der Bedarf an finanziellen und personellen Ressourcen mit einem zunehmenden Grad des Schutzes oder der Differenzierung des Schutzes. Unter Berücksichtigung dieser Randbedingungen sollte festgelegt werden, ob ein Grundschutz, eine detaillierte Risikoanalyse oder ein kombinierter Ansatz durchgeführt werden soll (vgl. [Ned99, Seite 11ff.]). Im Folgenden wird von einer detaillierten Risikoanalyse ausgegangen.

Festlegung des Geltungsbereichs und Feststellung der Werte

Es sollte der Geltungsbereich definiert und die innerhalb dieses Geltungsbereichs zu schützenden Werte festgestellt werden. Dabei finden sich generell in allen Teilbereichen eines IT-Systems, also Hardware, Software, Daten und Personen (vgl. Unterabschnitt 2.1.1), Werte, die zu schützen sind.

Feststellung der Verwundbarkeiten

Bei der Feststellung der Verwundbarkeiten der ermittelten Werte ist es oft schwierig, keine entscheidenden Verwundbarkeiten zu übersehen. Um eine möglichst vollständige Aufzählung zu erhalten, empfiehlt es sich, einen systematischen Ansatz anzuwenden. Eine Möglichkeit für einen solchen systematischen Ansatz ist, die ermittelten Werte den im Unterabschnitt 2.1.3 aufgeführten Schutzklassen in einer Art Matrix gegenüber zu stellen und in die Felder dieser Matrix die Verwundbarkeiten einzutragen (vgl. [Kro01, Seite 42f.]).

Feststellung der Bedrohungen

Bei der Feststellung der Bedrohungen bestehen bezüglich der Ermittlung aller relevanten Bedrohungen ähnliche Probleme wie bei der Feststellung der Verwundbarkeiten. Für einen systematischen Ansatz empfiehlt sich eine Einteilung der Bedrohungen in verschiedene

Klassen (vgl. [Øln94, Seite 631]). Eine Möglichkeit der Einteilung ist die im Unterabschnitt 2.1.2 aufgezeigte, von der BSI veröffentlichte Aufteilung in fünf Gefährdungskataloge (vgl. [BSI01, Gefährdungskataloge]).

Risikoanalyse

Das Ziel einer Risikoanalyse ist es, eine Abschätzung darüber zu entwickeln, welche Auswirkungen (**Schäden**) sicherheitsrelevante Ereignisse (**Vorfälle**) nach sich ziehen können (**Risikobewertung**). Generell wird dazu für alle sicherheitsrelevanten Ereignisse, die sich aus den festgestellten Verwundbarkeiten und Bedrohungen ergeben können, das daraus resultierende Schadensmaß und die Eintrittswahrscheinlichkeit abgeschätzt und diese Größen z.B. multiplikativ verknüpft (vgl. [Ned99, Seite 13f.]). Bei beiden Größen können sowohl kardinale als auch ordinale Ansätze eingesetzt werden. Beide Ansätze sollen hier am Beispiel der Abschätzung des Schadensmaßes angedeutet werden:

- Kardinaler Ansatz: Es wird der entstehende Schadenswert, bestehend aus materiellen und immateriellen Schäden, abgeschätzt (vgl. [Gro99, Seite 62]).
- Ordinaler Ansatz: Es werden Schadensklassen definiert, die Bereiche von Schadenswerten abdecken (z.B. Klasse 1: 10–100 Euro, Klasse 2: 100–1000 Euro, usw.), und die sicherheitsrelevanten Ereignisse diesen Schadensklassen zugeordnet (vgl. [Ned99, Seite 14]).

Festlegung und Bewertung von Maßnahmen und Festlegung von Verantwortlichkeiten

Mit den bei der Risikoanalyse ermittelten Abschätzungen kann für die einzelnen sicherheitsrelevanten Ereignisse festgelegt werden, welche Relevanz sie haben und wie viel in Schutzmaßnahmen investierter Aufwand ein sinnvolles Maß darstellt. So hat die Abwehr von Vorfällen, die eine hohe Eintrittswahrscheinlichkeit haben und dabei auch ein hohes Maß an Schäden verursachen können, sicher eine höhere Priorität als die Abwehr von selteneren und mit geringeren Schadensausmaßen behafteten Vorfällen. Ferner ist für die Abwehr der erstgenannten Vorfälle ein höherer Aufwand zu rechtfertigen.

Grundsätzlich sollten Maßnahmen zur Vorbeugung vor Vorfällen, Erkennung von Vorfällen und zur Wiederherstellung nach Vorfällen festgelegt werden (vgl. [Øln94]). Dabei ist eine Bewertung ihrer Wirkung (welche Risiken werden verringert und wie sehr) und der Verhältnismäßigkeit (Kosten, Wartbarkeit, Benutzbarkeit vs. erreichten Schutz) durchzuführen. Es sind Personen zu benennen, die für die Durchsetzung und die Überprüfung der Maßnahmen verantwortlich sind.

Feststellung des verbleibenden Restrisikos

Es sollten Abschätzungen darüber gemacht werden, wie hoch die verbleibenden Restrisiken sind. Dazu sind einerseits die verbleibenden Risiken bei Einsatz der Schutzmaßnahmen, andererseits aber auch neue, durch die Verwundbarkeiten der Maßnahmen bedingte Risiken

zu betrachten. Entspricht das verbleibende Risiko nicht dem zu erzielenden Schutzniveau, müssen die Schutzmaßnahmen überarbeitet oder die Erwartungen an das zu erzielende Schutzniveau korrigiert werden (vgl. in Abbildung 2.1 die auf der linken Seite eingezeichneten Pfeile).

Implementierung, Bekanntmachung, Durchsetzung und Überprüfung

Außer die in der IT-Sicherheitspolitik festgelegten Maßnahmen zu implementieren, ist es notwendig, die Ziele der IT-Sicherheitspolitik bekannt zu machen und die Betroffenen über die Maßnahmen und insbesondere auch über die Gründe für den Einsatz der Maßnahmen zu informieren. Derartige Schulungen sollten regelmäßig wiederholt werden, da über die Zeit oft eine „Abstumpfung“ zu beobachten ist. Schließlich ist es notwendig, verschiedene Teile der IT-Sicherheitspolitik, insbesondere die festgelegten Maßnahmen, auf ihre Auswirkungen hin zu überprüfen und ggf. zu überarbeiten. („Controlling“) (vgl. [Gro99, Seite 66]). Dies wird in der Abbildung 2.1 durch die auf der rechten Seite eingezeichneten Pfeile angedeutet.

2.3 Abgrenzung des Begriffs Nutzer

In diesem Abschnitt soll eine Abgrenzung der verschiedenen, innerhalb dieser Arbeit betrachteten Personengruppen erfolgen. Dabei soll insbesondere herausgearbeitet werden, welche Personen als Nutzer zu betrachten sind, und welche Fähigkeiten und Verhaltensweisen bei den verschiedenen Personengruppen angenommen werden können.

Dazu soll zunächst eine grobe Unterscheidung zwischen Personengruppen innerhalb einer Organisation und Externen erfolgen. Aufgrund des hier betrachteten Zusammenhangs soll diese Unterscheidung anhand der Zugriffsmöglichkeiten, die Personen auf das IT-System einer Organisation haben, durchgeführt werden. Als Personengruppen innerhalb einer Organisation sollen solche verstanden werden, die aufgrund ihres Verhältnisses zur Organisation (z.B. angestellt, Eigentümer) einen autorisierten Zugriff auf das IT-System haben. Hierbei sollen die Gruppen Nutzer, Administratoren und Management zueinander abgegrenzt werden. Als Externe sollen solche Personen verstanden werden, die keinen oder im Ausnahmefall einen stark beschränkten Zugriff auf das IT-System haben. Als hier zu betrachtende Externe werden externe Berater und Dritte unterschieden. Des Weiteren soll eine Unterscheidung in kooperative und nicht-kooperative Personen durchgeführt werden.

Personengruppen innerhalb einer Organisation

- Nutzer
  Nutzer haben als Angehörige (sehr oft Angestellte) einer Organisation Zugriff auf das IT-System der Organisation und verwenden dieses zur Verrichtung ihrer Aufgaben. Dabei ist die Gewährleistung des Betriebs der IT-Systeme generell nicht Teil ihrer Aufgaben (im Gegensatz hierzu siehe Administratoren). Grundsätzlich muss davon ausgegangen werden, dass die Nutzer auch die IT-Sicherheit nicht als Bestandteil ihrer Aufgaben sehen, sondern im schlimmsten Fall als eine möglichst zu umgehende

Behinderung ihrer Arbeitsprozesse. Das Wissen über die IT-Systeme im Allgemeinen und der IT-Sicherheit im Speziellen muss bei Nutzern als sehr unterschiedlich angenommen werden.

Im Rahmen dieser Arbeit werden Nutzer in Bezug auf IT-Sicherheitspolitiken aus verschiedenen Sichten betrachtet. Einerseits erfolgt eine Betrachtung der Nutzer als aktiver Teil bei der Erstellung einer IT-Sicherheitspolitik (vgl. Kapitel 3), andererseits als Gegenstand der IT-Sicherheitspolitik, z.B. als Verwundbarkeit oder Bedrohung (vgl. Kapitel 4), aber auch bei den Schutzmaßnahmen (vgl. Kapitel 5) oder der Durchsetzung dieser Schutzmaßnahmen (vgl. Kapitel 8).

- Administratoren
  Administratoren haben ebenso wie Nutzer Zugriff auf das IT-System. Ihr Aufgabenbereich ist die Gewährleistung des Betriebs der IT-Systeme. Es soll angenommen werden, dass Administratoren grundsätzlich ein ausgeprägtes Wissen im Bereich von IT-Systemen haben. Im speziellen Fall der IT-Sicherheit muss aber auch von solchen Administratoren ausgegangen werden, die ihre Aufgabenstellung ausschließlich in der Bereitstellung von Diensten, nicht aber in der Absicherung dieser sehen. Da IT-Systeme sehr komplex sind, muss davon ausgegangen werden, dass auch Administratoren Fehler machen bzw. Unterlassungen begehen können.

- Management
  Das Management ist grundsätzlich eine spezielle Gruppe von Nutzern, die hier hervorgehoben wird, da sie Entscheidungsträger sind. Es muss davon ausgegangen werden, dass Manager oft Betriebswirte sind, bei denen kein ausgeprägtes Wissen über IT-Sicherheit vorausgesetzt werden kann.

Personengruppen außerhalb der betrachteten Organisation

- Externe Berater
  Externe Berater werden im Allgemeinen, oft zeitlich begrenzt, als Spezialisten für bestimmte Aufgaben in der Organisation eingesetzt. Ihr Aufgabenbereich kann z.B. IT-Systeme, IT-Sicherheit oder damit im Zusammenhang stehende Bereiche wie Datenschutz o.ä. sein. Es ist denkbar, dass externen Beratern zur Erfüllung ihrer Aufgaben ein Zugriff auf das IT-System gewährt wird, der im Allgemeinen zeitlich und bzgl. der Rechte stark eingeschränkt ist.

- Dritte
  Im Gegensatz zu den bisher betrachteten Personengruppen, stehen Dritte in keiner direkten Beziehung zu der betrachteten Organisation. Vorwiegend sollen hier Dritte betrachtet werden, die einer Organisation Schaden zufügen wollen (Angreifer, vgl. Unterabschnitt 2.1.2). Es soll davon ausgegangen werden, dass sie keinen autorisierten Zugriff auf das IT-Systemen der Organisation haben. Es können keine Annahmen über das Wissen über IT-Systeme und IT-Sicherheit gemacht werden, d.h. es müssen sowohl unbedarfte als auch sehr versierte Personen angenommen werden.

Unterscheidung zwischen kooperativen und nicht-kooperativen Personen

Bei den für die Organisation arbeitenden Personen kann zwischen kooperativen und nicht-kooperativen unterschieden werden. Dabei soll davon ausgegangen werden, dass nicht-kooperative Personen mit Vorsatz gegen die IT-Sicherheitspolitik handeln, indem sie z.B. Schutzmaßnahmen umgehen oder im Extremfall Angreifer sind. Gründe für Angriffe können sein:

- Schaffung eines (materiellen) Vorteils für sich oder andere,
- Rache an der Organisation, z.B. aus Unzufriedenheit,
- oder auch politisch bedingte Beweggründe.

2.4 Zusammenfassung

In diesem Kapitel wurden für diese Arbeit relevante Begriffe und Sachverhalte eingeführt. Dazu wurde im Abschnitt 2.1 aufgezeigt, dass unter einem IT-System ein System, bestehend aus Hardware, Software, Daten und Nutzern, zur Aufbewahrung, Übertragung oder Verarbeitung von informationstragenden Daten verstanden werden soll. Es wurde ausgeführt, dass IT-Systeme Risiken ausgesetzt sind, die durch die Möglichkeit des Zusammentreffens von Verwundbarkeiten des IT-Systems und Bedrohungen aus der Umgebung entstehen. Ferner wurde gezeigt, dass zur Verringerung der Risiken physikalische, organisatorische oder technische Schutzmaßnahmen eingesetzt werden können, die präventiv, detektiv oder korrektiv wirken. Dabei wurde zwischen Schutzmaßnahmen im Rahmen eines Grundschutzes und eines individuellen Schutzes unterschieden. Als Schutzziele wurden Vertraulichkeit, Integrität und Verfügbarkeit genannt.

Dem Folgend wurde im Abschnitt 2.2 festgelegt, dass im Rahmen dieser Arbeit IT-Sicherheitspolitiken betrachtet werden sollen, die Handlungen von Personen betreffen. Es wurden verschiedene Formen von IT-Sicherheitspolitiken unterschieden: implizite, die in Form von implementierten Sicherheitsmechanismen oder im Bewusstsein des Verantwortlichen existieren können, und explizite, die in Form eines oder mehrerer Dokumente oder in Form eines „Slogan“ vorliegen können. Als Inhalt einer IT-Sicherheitspolitik wurden Geltungsbereich, Ziele, zugelassene Handlungen, Maßnahmen, Durchsetzung, Vorfallsbehandlung, Weiterentwicklung und Dokumentation der Erstellung aufgeführt. Anschließend wurden Phasen der Erstellung einer IT-Sicherheitspolitik benannt und ausgeführt.

Im Abschnitt 2.3 wurde eine Differenzierung verschiedener, für die folgenden Betrachtungen relevanter Personengruppen vorgenommen. Dazu wurde zunächst zwischen internen und externen Personengruppen unterschieden. Als interne Personengruppen wurden Nutzer, Administratoren und das Management betrachtet. Als externe Personengruppen Berater und Dritte. Abschließend wurde aufgezeigt, dass Personen, die mit Vorsatz gegen die IT-Sicherheitspolitik verstoßen, als nicht-kooperative Personen bezeichnet werden und dass in diesem Fall Angreifer und Personen, die Sicherheitsmaßnahmen umgehen, unterschieden werden können.

Kapitel 3

Einbeziehung der Nutzer bei der Erstellung von IT-Sicherheitspolitiken

- Ziel:
  Es sollen die Auswirkungen verschiedener Arten der Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik betrachtet werden.
- Vorgehen:
  1. Betrachtung von die Art der Einbeziehung der Nutzer beeinflussenden Randbedingungen
  2. Betrachtung der bei der Erstellung einer IT-Sicherheitspolitik verfolgten Ziele und die Auswirkungen verschiedener Arten der Einbeziehung der Nutzer auf diese
  3. Betrachtung verschiedener Arten der Einbeziehung der Nutzer

In diesem Kapitel sollen Betrachtungen zu den Auswirkungen einer Einbeziehung der Nutzer bei der Erstellung von IT-Sicherheitspolitiken durchgeführt werden. Die Eingrenzung der hier durchzuführenden Betrachtungen auf die Gruppe der Nutzer erfolgt aufgrund der Themenstellung dieser Arbeit.

Zunächst sollen im Abschnitt 3.1 mögliche Randbedingungen betrachtet werden, die die Art der Einbeziehung der Nutzer beeinflussen können. Anschließend soll im Abschnitt 3.2 diskutiert werden, welche Ziele mit der Erstellung einer IT-Sicherheitspolitik verbunden sein können und wie sich verschiedene Arten der Einbeziehung der Nutzer bei der Erstellung auf das Erreichen dieser Ziele auswirken können. Im Abschnitt 3.3 sollen dann beispielhaft drei Arten der Einbeziehung der Nutzer betrachtet werden. Abschließend soll im Abschnitt 3.4 eine Zusammenfassung gegeben werden.

3.1 Betrachtung möglicher Randbedingungen

In diesem Abschnitt sollen mögliche Randbedingungen betrachtet werden, die die Art, in der die Nutzer bei der Erstellung einer IT-Sicherheitspolitik einbezogen werden, beeinflussen oder im Extremfall sogar bestimmen können. Eine Betrachtung der Randbedingungen ist daher wichtig, da diese oft gar nicht oder nur schwer beeinflusst werden können und daher Fälle denkbar sind, in denen die durch die Randbedingungen bestimmte Vorgehensweise gewählt werden muss, obwohl sie nicht der aufgrund der Zielvorgaben zu wählenden Vorgehensweise entspricht. Es soll hier eine Differenzierung zwischen Randbedingungen vorgenommen werden, die durch die Umwelt vorgegeben werden, die durch Interaktion mit der Umwelt entstehen und die ihre Ursachen innerhalb einer Organisation haben.

- Randbedingungen, die durch die Umwelt vorgegeben sind, können Gesetze und Verordnungen sein. Durch Gesetze oder Verordnungen kann z.B. in bestimmten Fällen die Einbeziehung der Nutzer oder einer Vertretung der Nutzer (Betriebsräte oder Ähnliches) vorgeschrieben sein.

- Randbedingungen, die durch die Interaktion mit der Umwelt entstehen, können bestehende Verträge sein. So kann z.B. generell eine Einbeziehung der Nutzer in Tarifverträgen vorgesehen sein.

- Randbedingungen, die ihre Ursachen innerhalb einer Organisation haben, können durch eine Firmenphilosophie bzw. Unternehmenskultur begründet sein. So kann eine Firmenphilosophie sein, dass Entscheidungen dieser Art grundsätzlich nur vom Management getroffen werden und eine Einbeziehung der Nutzer dabei nicht erfolgt. Im Kontrast dazu steht eine Unternehmenskultur, die außer durch andere Maßnahmen durch eine Einbeziehung der Nutzer bei allen weitreichenden Fragen zu einer stärkeren Identifikation mit der Organisation führen soll.

3.2 Betrachtung von Auswirkungen der Einbeziehung der Nutzer auf Ziele der Erstellung

Bei der Erstellung einer IT-Sicherheitspolitik können verschiedene Ziele verfolgt werden. Beispiele sind, dass die Erstellung effizient erfolgen soll, die entwickelte IT-Sicherheitspolitik gut durchsetzbar oder die in der IT-Sicherheitspolitik aufgeführten Maßnahmen angemessen sein sollen. In diesem Abschnitt sollen mögliche Auswirkungen verschiedener Arten der Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik auf diese Ziele betrachtet werden. Dazu sollen zunächst mögliche, bei der Erstellung einer IT-Sicherheitspolitik zu erreichende Ziele aufgezeigt werden (vgl. Unterabschnitt 3.2.1). Anschließend soll betrachtet werden, welche Arten der Einbeziehung der Nutzer das Erreichen dieser Ziele unterstützen (vgl. Unterabschnitt 3.2.2).

3.2.1 Erarbeitung möglicher Ziele

Im Folgenden sollen verschiedene Ziele aufgezeigt werden, die bei der Erstellung einer IT-Sicherheitspolitik verfolgt werden können. Dabei soll eine Differenzierung der Ziele in die folgenden drei Bereiche erfolgen:

- Ziele bzgl. des Prozesses der Erstellung einer IT-Sicherheitspolitik
- Ziele bzgl. der Durchsetzbarkeit der zu erstellenden IT-Sicherheitspolitik
- Ziele bzgl. der Wirksamkeit der in der IT-Sicherheitspolitik festgelegten Maßnahmen

Betrachtung von Zielen bzgl. des Prozesses der Erstellung

Bezüglich des Prozesses der Erstellung einer IT-Sicherheitspolitik soll als Ziel angenommen werden, dass dieser möglichst effizient durchgeführt werden soll. Im Allgemeinen bedeutet dies, dass bei der Erstellung möglichst wenige Ressourcen wie z.B. Personal und Zeit benötigt werden sollen.

Betrachtung von Zielen bzgl. der Durchsetzbarkeit

Um eine bessere Durchsetzbarkeit einer IT-Sicherheitspolitik zu erreichen, ist es oft sinnvoll, bereits bei der Erstellung die bei der Durchsetzung bestehenden Ziele zu berücksichtigen. Im Folgenden sollen einige Ziele aufgeführt werden, die bei der Durchsetzung bestehen können:

- Angemessene Implementierung der Maßnahmen
  Die in der IT-Sicherheitspolitik festgelegten Maßnahmen müssen in angemessener Weise implementiert werden, damit der bei der Erstellung der IT-Sicherheitspolitik angenommene Wirkungsgrad nicht durch Implementierungsfehler gemindert wird.

- Gute Verbreitung der Informationen über die Maßnahmen
  Alle Betroffenen sollten möglichst gut über die Maßnahmen, die sich direkt auf ihre Arbeitsabläufe auswirken, informiert sein. Dies gilt sowohl für die Existenz dieser Maßnahmen als auch für das im Rahmen dieser Maßnahmen von ihnen erwartete Verhalten.

- Hohe Akzeptanz für die Durchführung der Maßnahmen
  Bei allen Betroffenen sollte eine möglichst große Akzeptanz für die Durchführung der in der IT-Sicherheitspolitik festgelegten Maßnahmen entwickelt werden. Besteht diese Akzeptanz nicht, so können oft Versuche beobachtet werden, diese zu umgehen. Dies trifft auf die Nutzer, aber auch auf die Administratoren und das Management zu, bei denen sich unter Umständen die Meinung bilden kann, dass die Maßnahmen für Personen in besonderen Positionen nicht gelten.

Betrachtung von Zielen bzgl. der Wirksamkeit

Bezüglich der Wirksamkeit soll als Ziel die Angemessenheit der in einer IT-Sicherheitspolitik festgelegten Maßnahmen angenommen werden. Unter Angemessenheit soll hier ein gutes Verhältnis zwischen dem erzielten Schutz gegen existierende Bedrohungen zu dem durch die Maßnahmen erzeugten Aufwand verstanden werden. Um eine bessere Angemessenheit von Maßnahmen zu erreichen, müssen im Allgemeinen die folgenden Punkte auch bereits bei der Erstellung einer IT-Sicherheitspolitik beachtet werden:

- Auswahl angemessener Maßnahmen
  Um eine Auswahl angemessener Maßnahmen zu erreichen, muss u.a. die Umgebung, in der die Maßnahmen eingesetzt werden sollen, und die Wirkung bzw. der Wirkungsgrad der Maßnahmen berücksichtigt werden.

- Angemessene Durchsetzung der Maßnahmen
  Die Durchsetzung wurde bereits behandelt (siehe oben).

- Fortschreibung der IT-Sicherheitspolitik
  Eine IT-Sicherheitspolitik muss fortgeschrieben werden, um z.B. an Verwundbarkeiten oder Bedrohungen angepasst zu werden, die bei der Erstellung nicht berücksichtigt wurden. Bereits bei der Erstellung einer IT-Sicherheitspolitik sollten Ereignisse festgelegt werden, die eine Anpassung erfordern (vgl. Unterabschnitt 2.2.3).

3.2.2 Untersuchung der Auswirkungen verschiedener Arten der Einbeziehung der Nutzer

In diesem Unterabschnitt soll betrachtet werden, welche Auswirkungen verschiedene Arten der Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik auf die Erreichung der im vorhergehenden Unterabschnitt 3.2.1 aufgeführten Ziele haben können. Dabei soll wiederum in Ziele bzgl. des Prozesses der Erstellung, bzgl. der Durchsetzbarkeit und bzgl. der Wirksamkeit unterschieden werden.

Auswirkungen auf Ziele bzgl. des Prozesses der Erstellung

Bezüglich des Prozesses der Erstellung einer IT-Sicherheitspolitik soll als Ziel angenommen werden, dass dieser Prozess möglichst effizient durchgeführt werden soll (vgl. Unterabschnitt 3.2.1). Es kann grundsätzlich angenommen werden, dass eine Vergrößerung der Gruppe, der bei der Erstellung Beteiligten, diesem Ziel entgegenwirkt. Dies kann u.a. mit längeren Kommunikations- und Entscheidungswegen begründet werden. Ausnahmen können sich ergeben, wenn die Gruppe so klein gewählt wird, dass nicht mehr alle notwendigen Kenntnisse innerhalb der Gruppe vorhanden sind und daher eine Einbeziehung Externer oder eine Einarbeitung von Gruppenmitgliedern notwendig ist. Für die Art der Einbeziehung der Nutzer bedeutet dies, dass das Ziel einer möglichst effizienten Erstellung oft am besten erfüllt wird, wenn keine Einbeziehung der Nutzer oder eine eingeschränkte Einbeziehung der Nutzer z.B. über Vertreter erfolgt.

Auswirkungen auf Ziele bzgl. der Durchsetzbarkeit

Im Folgenden soll betrachtet werden, welche Auswirkungen die Einbeziehung von Nutzern bei der Erstellung einer IT-Sicherheitspolitik auf die Ziele bzgl. der Durchsetzung haben kann.

- Angemessene Implementierung der Maßnahmen
  Es kann davon ausgegangen werden, dass die Implementierung von in der IT-Sicherheitspolitik festgelegten physikalischen und technischen Maßnahmen im Allgemeinen von Spezialisten durchgeführt wird und daher die Art der Einbeziehung der Nutzer bei der Erstellung der IT-Sicherheitspolitik keine Auswirkungen auf die Implementierung dieser Maßnahmen hat. Die Implementierung organisatorischer Maßnahmen besteht vorwiegend aus der Informierung der Betroffenen und der Schaffung einer Akzeptanz für die Maßnahmen. Beides wird im Folgenden behandelt.

- Gute Verbreitung der Informationen über die Maßnahmen
  Wären Nutzer bei der Erstellung der IT-Sicherheitspolitik einbezogen, so würden sie bereits während dieses Prozesses auch über die Maßnahmen informiert werden. Es ist aber zu beachten, dass die Nutzer neben den für sie relevanten auch andere Informationen erhalten würden. Ferner werden die Informationen grundsätzlich nicht in einer für die Nutzer adäquaten Art aufbereitet sein. Die Nutzer müssten daher selbst entscheiden, welche Informationen für sie relevant sind und wie sie ihre Arbeitsabläufe anzupassen haben. Da nicht zu erwarten ist, dass dies von allen Nutzern geleistet werden kann, ist eine Aufbereitung und Verbreitung der Informationen z.B. durch Schulungen oder Dokumente auch in diesem Fall notwendig. Es kann aber angenommen werden, dass bei einer Einbeziehung der Nutzer bei vielen ein tieferes Verständnis vermittelt werden kann, als es z.B. bei Schulungen möglich wäre, so dass eine Einbeziehung hier von Vorteil sein kann.

- Hohe Akzeptanz für die Durchführung der Maßnahmen
  Zunächst soll betrachtet werden, aus welchen Gründen die Schaffung einer Akzeptanz für die Durchführung der Maßnahmen notwendig ist. Dann soll aufgezeigt werden, auf welche Weise diese Akzeptanz auch im Rahmen der Erstellung einer IT-Sicherheitspolitik erreicht werden kann.

  Die Notwendigkeit eine möglichst hohe Akzeptanz für die Durchführung der in der IT-Sicherheitspolitik festgelegten Maßnahmen zu erreichen, ergibt sich aufgrund von sehr oft zu beobachtenden grundsätzlichen Widerständen gegen Änderungen innerhalb von Organisationen, die zur Umgehung der Maßnahmen führen können. Als Gründe für diese Widerstände können neben evtl. auftretenden objektiven Verschlechterungen (z.B. bei Entlassungen) auch die Folgenden angenommen werden (vgl. [Sch99, Seite 485ff.]):

  - Angst vor persönlichen Nachteilen (z.B. Kompetenz- und Prestigeverlust, soziale Verluste bei anderen Gruppenzusammensetzungen)

– die Befürchtung das Gewohnte und Vertraute (z.B. bisher erfolgreich praktizierte Arbeitsweisen) zu verlassen und sich einer Situation der Ungewissheit auszusetzen

Um eine Akzeptanz für die durch die Durchsetzung der Maßnahmen bedingten Veränderungen zu erreichen, ist es oft notwendig, ein Verständnis dafür zu entwickeln, welche Ursachen für die Veränderungen bestehen und welche Auswirkungen die Maßnahmen auf diese Ursachen haben. Grundsätzlich wird die Ansicht vertreten, dass eine aktive und kooperative Einbeziehung der Betroffenen größere Erfolge erzielt als eine Vorstellung durch Vorträge (vgl. [Sch99, Seite 489f.]). Um eine möglichst hohe Akzeptanz zu schaffen, kann es daher sinnvoll sein, die Nutzer bereits bei der Erstellung einer IT-Sicherheitspolitik einzubeziehen.

Grundsätzlich kann also angenommen werden, dass die Ziele bzgl. der Durchsetzung einer IT-Sicherheitspolitik durch eine breite Einbeziehung der Nutzer unterstützt werden können. Bei der vorhergehenden Betrachtung der Auswirkungen auf Ziele bzgl. des Prozesses der Erstellung wurde im Gegensatz dazu festgestellt, dass eine geringe Einbeziehung der Nutzer die dort betrachteten Ziele unterstützen würde. Es zeigt sich also schon hier, dass es keine allgemein gültige optimale Art der Einbeziehung gibt, sondern im konkreten Fall eine Abwägung notwendig ist.

Auswirkungen auf Ziele bzgl. der Wirksamkeit

Bei der Wirksamkeit einer IT-Sicherheitspolitik soll als Ziel die Angemessenheit der in ihr festgelegten Maßnahmen angenommen werden (vgl. Unterabschnitt 3.2.1). Im Folgenden soll aufgezeigt werden, welche Ursachen dazu führen können, dass Maßnahmen nicht angemessen sind. Ferner soll betrachtet werden, wie sich verschiedene Arten der Einbeziehung der Nutzer auf diese Ursachen auswirken können.

- Auswahl nicht angemessener Maßnahmen
  Ursachen dafür, dass eine Auswahl nicht angemessener Maßnahmen erfolgt, können falsche Annahmen bzgl. der Umgebung, in der die Maßnahmen eingesetzt werden sollen, oder falsche Annahmen bzgl. der Wirkung oder des Wirkungsgrads der ausgewählten Maßnahmen sein. Falsche Annahmen bzgl. der Umgebung können ihre Ursache z.B. in Fehlern bei der Feststellung der Verwundbarkeiten und den Bedrohungen bzw. der Risikoanalyse haben. So können vorhandene Verwundbarkeiten und Bedrohungen nicht erkannt oder das durch erkannte Verwundbarkeiten und Bedrohungen entstehende Risiko falsch eingeschätzt werden. Dies kann u.a. geschehen, wenn falsche Annahmen über die Arbeitsabläufe der Nutzer gemacht werden.

  Hierzu sei folgendes Beispiel aufgeführt: Bei der Erstellung der IT-Sicherheitspolitik wird angenommen, dass die Nutzer ihre Passworte geheim halten. Tatsächlich tauschen die Nutzer aber ihre Passworte aus, um auch dann auf Daten anderer Nutzer zugreifen zu können, wenn diese im Urlaub oder krank sind. Eine in einem derartigen Fall nicht berücksichtigte Bedrohung kann z.B. sein, dass Nutzer einen Missbrauch

der Ressourcen dadurch verschleiern können, dass sie diesen mit wechselnden Zugängen anderer Nutzer durchführen.

Falsche Annahmen bzgl. des durch die Maßnahmen erzielbaren Schutzes können oft auf eine „Technik-Gläubigkeit“ zurückgeführt werden. Dabei wird oft davon ausgegangen, dass sich Probleme, die durch den Einsatz von Technik entstehen und durch organisatorische Maßnahmen nicht beherrscht werden können, durch den Einsatz weiterer technischer Maßnahmen beherrschen lassen.

Werden die Nutzer bei der Erstellung einer IT-Sicherheitspolitik einbezogen, so ist es grundsätzlich möglich, die Umgebung (z.B. bestehende Arbeitsabläufe) besser einzuschätzen. Es muss aber beachtet werden, dass bei der Einbeziehung der Nutzer eine zu sehr an den Anwendungen orientierte Blickrichtung an Stelle der „Technik-Gläubigkeit“ treten kann. Diese kann dann ebenfalls zu einer Auswahl von nicht angemessenen Maßnahmen führen.

- Mangelnde Fortschreibung der IT-Sicherheitspolitik
  Die Fortschreibung einer IT-Sicherheitspolitik ist im Allgemeinen ein organisatorisches Problem, auf das die Einbeziehung von Nutzern bei der Erstellung der IT-Sicherheitspolitik grundsätzlich keinen Einfluss hat.

3.3 Betrachtung verschiedener Arten der Einbeziehung

In diesem Abschnitt sollen exemplarisch die folgenden drei Arten der Einbeziehung von Nutzern betrachtet werden:

1. „Diktatur“
   Es erfolgt keine Einbeziehung der Nutzer, die IT-Sicherheitspolitik wird vom Management „diktiert“ (vgl. Unterabschnitt 3.3.1).

2. „Demokratur“[1]
   Die Nutzer werden zwar bei der Erstellung einbezogen, Entscheidungen werden aber vom Management gefällt (vgl. Unterabschnitt 3.3.2).

3. „Demokratie“
   Es werden alle Beteiligten einbezogen, ferner werden auch die Entscheidungen von allen Beteiligten gemeinsam gefällt, die IT-Sicherheitspolitik wird in einem „demokratischen“ Verfahren entwickelt (vgl. Unterabschnitt 3.3.3).

3.3.1 „Diktatur“

In diesem Fall soll angenommen werden, dass die IT-Sicherheitspolitik vom Management diktiert wird, ohne dass eine Einbeziehung der Nutzer bei der Erstellung erfolgt. Die Erstel-

[1] Das Wort „Demokratur“ ist eine von Herrn Brunnstein, dem Erstbetreuer dieser Arbeit, vorgeschlagene Zusammensetzung aus den Worten „**Demokr**atie“ und „Dikt**atur**“.

lung wird hierbei oft nicht durch das Management, sondern durch eine vom Management bestimmte Menge von Spezialisten (z.B. Administratoren, externe Berater) erfolgen.

Bei einem solchen Vorgehen wäre nur eine geringe Anzahl Personen einbezogen. Das kann kurze Kommunikations- und Entscheidungswege und damit eine sehr effiziente Erstellung zur Folge haben. Da die Nutzer nicht einbezogen werden, ist es allerdings notwendig, sie bei der Durchsetzung durch Maßnahmen zur Bekanntmachung wie Schulungen oder Dokumente (vgl. Kapitel 8) über die IT-Sicherheitspolitik zu informieren. Es ist wahrscheinlich, dass bei den Nutzern eine geringe Akzeptanz für die Durchführung der in der IT-Sicherheitspolitik festgelegten Maßnahmen bestehen wird. Ein sehr ausschlaggebender Grund hierfür könnte sein, dass sie „nicht gefragt worden sind“. Ferner besteht die Gefahr, dass die IT-Sicherheitspolitik zu wenig an die Bedürfnisse der Nutzer angepasst ist und die in ihr festgelegten Maßnahmen daher ihre Arbeitsabläufe behindern.

3.3.2 „Demokratur“

In diesem Fall soll angenommen werden, dass eine Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik erfolgt, die Entscheidungen aber vom Management getroffen werden. Der Grad der Einbeziehung kann in diesem Fall stark differenziert werden. Einerseits kann die Einbeziehung nur aus einem Informationsfluss von den Nutzern in Richtung des Managements bestehen, indem z.B. Fragebögen oder Interviews genutzt werden, um Sachverhalte wie Arbeitsabläufe zu ermitteln. Andererseits kann auch ein Informationsfluss in beide Richtungen angenommen werden, indem z.B. Diskussionsrunden geführt werden, in denen die Nutzer über die IT-Sicherheitspolitik informiert werden und ihre Bedenken und Wünsche äußern können.

Da hier viele Personen einzubeziehen sind, ist grundsätzlich mit mehr Aufwand bei der Erstellung einer IT-Sicherheitspolitik zu rechnen. Um auch in diesem Fall eine effiziente Erstellung zu gewährleisten, ist es notwendig, eine Planung durchzuführen, in der bestimmt wird, wann von welchen Personen Informationen erhoben bzw. an sie weiter gegeben werden sollen. Grundsätzlich bestehen hier gute Möglichkeiten, bereits bei der Erstellung die Nutzer zu informieren und bei ihnen Akzeptanz zu entwickeln.

3.3.3 „Demokratie“

In diesem Fall soll davon ausgegangen werden, dass alle Betroffenen bei der Erstellung einer IT-Sicherheitspolitik einbezogen werden und insbesondere auch alle an Entscheidungen beteiligt sind. Dabei können mehrere Differenzierungen vorgenommen werden. So kann zwischen Konsens- oder Mehrheitsentscheidungen unterschieden werden, die Stimmen können gleich oder ungleich gewichtet werden und es kann ein Veto-Recht vorgesehen sein.

Es kann davon ausgegangen werden, dass ein solches Vorgehen einen sehr hohen Aufwand nach sich ziehen würde. In Bezug auf die Durchsetzung können generell zwei unterschiedliche Auswirkungen angenommen werden. Einerseits ist es denkbar, dass die breite Einbeziehung zu einer guten Verbreitung von Informationen und zu einer hohen Akzeptanz bei den Nutzern führen kann. Andererseits besteht die Gefahr, dass sich Nutzer aus dem

Prozess der Erstellung ausgrenzen. Ursachen hierfür können z.B. sein, dass ihnen der Aufwand zu hoch ist oder dass ihre Vorschläge nicht aufgegriffen wurden. Ferner muss beachtet werden, dass die Wirkung der festgelegten Maßnahmen u.U. nicht angemessen ist, da bei der großen Anzahl von Entscheidungsträgern sehr unterschiedliche Interessen anzunehmen sind. Diese können dazu führen, dass man sich bei der Findung einer gemeinsamen Position auf den oft nicht angemessenen „kleinsten gemeinsamen Nenner“ einigen muss.

3.4 Zusammenfassung

In diesem Kapitel wurde die Einbeziehung der Nutzer bei der Erstellung einer IT-Sicherheitspolitik betrachtet. Es wurde zunächst im Abschnitt 3.1 aufgezeigt, dass es verschiedene Randbedingungen gibt, die die Art der Einbeziehung der Nutzer beeinflussen oder sogar bestimmen können. Dabei wurde unterschieden in Randbedingungen, die durch die Umwelt vorgeben sind (z.B. Gesetze und Verordnungen), Randbedingungen, die durch die Interaktion mit der Umwelt entstehen (z.B. Verträge), und Randbedingungen, die ihre Ursachen innerhalb einer Organisation haben (z.B. Firmenphilosophie oder Unternehmenskultur).

Dann wurden im Abschnitt 3.2 Ziele aufgezeigt, die mit der Erstellung einer IT-Sicherheitspolitik verfolgt werden können, und es wurde betrachtet, wie sich verschiedene Arten der Einbeziehung auf diese Ziele auswirken können. Dabei wurde unterschieden in Ziele in Bezug auf den Prozess der Erstellung (Effizienz), die Durchsetzung (Implementierung, Information und Akzeptanz) und die Wirksamkeit (Angemessenheit der Maßnahmen). Es konnte festgestellt werden, dass sich bzgl. der Ziele der Erstellung eine geringe und bzgl. der Ziele der Durchsetzung eine möglichst breite Einbeziehung der Nutzer positiv auswirken würde. Bei den Zielen bzgl. der Wirksamkeit wurde festgestellt, dass beide Extreme zu Problemen führen können.

Abschließend wurden im Abschnitt 3.3 drei Arten der Einbeziehung (keine Einbeziehung, Einbeziehung aber keine Entscheidungsgewalt und Einbeziehung mit Entscheidungsgewalt) der Nutzer bei der Erstellung einer IT-Sicherheitspolitik betrachtet. Dabei wurde festgestellt, dass bei keiner Einbeziehung zwar eine effiziente Erstellung möglich ist, sich aber auch negative Effekte für die Durchsetzbarkeit und die Wirksamkeit ergeben können. Bei einer Einbeziehung der Nutzer, ohne dass sie Entscheidungen treffen dürfen, muss zwar auf der einen Seite von einem höheren Aufwand ausgegangen werden, es können sich aber auf der anderen Seite positive Auswirkungen auf die Durchsetzbarkeit und die Wirksamkeit ergeben. Werden die Nutzer mit einer Entscheidungsbefugnis einbezogen, so kann davon ausgegangen werden, dass der Aufwand weiter steigt und im schlimmsten Fall die grundsätzlich anzunehmenden positiven Auswirkungen auf die Durchsetzbarkeit und die Wirksamkeit u.U. durch Seiteneffekte eingeschränkt werden. Zusammenfassend kann festgestellt werden, dass die in diesem Kapitel durchgeführten Betrachtungen keinen allgemein gültigen Schluss über eine optimale Art der Einbeziehung von Nutzern zulassen. Vielmehr muss für den Einzelfall und im Extremfall sogar für die einzelnen Phasen der Erstellung überlegt werden, ob der Aufwand der Einbeziehung der Nutzer mit den Vorteilen bei der Durchsetzbarkeit und der Wirksamkeit in einem angemessenen Verhältnis steht.

Kapitel 4

Entwicklung von Szenarien

- Ziel:
  Entwicklung eines Katalogs von Szenarien, in denen Sicherheitsprobleme aufgezeigt werden, die von Nutzern verursacht oder beobachtet werden können.
- Vorgehen:
  1. Aufstellung von zwei Fallbeispielen für den Einsatz von IT-Systemen, anhand derer verschiedene Prinzipien der Sicherheit von IT-Systemen aufgezeigt werden sollen
  2. Aufstellung einer Systematik für die Auswahl der Szenarien
  3. Erarbeitung von Szenarien
  4. Einordnung der Szenarien in die Systematik

In diesem Kapitel sollen Szenarien entwickelt werden, die sicherheitsrelevante Ereignisse aufzeigen, an denen Nutzer direkt (z.B. als Verwundbarkeit oder Angreifer) oder indirekt (z.B. als Zeuge eines Vorfalls) beteiligt sind. Im folgenden Kapitel 5 sollen dann Schutzmaßnahmen aufgezeigt werden, die gegen diese sicherheitsrelevanten Ereignisse gerichtet sind, und bei denen eine aktive Einbeziehung der Nutzer erfolgt.

Zunächst sollen im Abschnitt 4.1 zwei Fallbeispiele aufgestellt und anhand dieser Fallbeispiele einige Prinzipien der Sicherheit von IT-Systemen erläutert werden. Dann soll im Abschnitt 4.2 eine Betrachtung verschiedener, bei der Auswahl der Szenarien zu berücksichtigender Aspekte erfolgen. Dazu sollen im Unterabschnitt 4.2.1 die Anforderungen ausgeführt werden, die an die zu entwickelnden Szenarien zu stellen sind, im Unterabschnitt 4.2.2 sollen dann die Rollen aufgezeigt werden, in denen Nutzer in den Szenarien auftreten können, und im Unterabschnitt 4.2.3 soll eine Aufstellung einer allgemeinen Verwundbarkeitsmatrix durchgeführt werden. Im Abschnitt 4.3 soll dann die Entwicklung der Szenarien erfolgen. Anschließend soll im Abschnitt 4.4 ein Überblick über die Einordnung der Szenarien in die aufgestellten Systematiken aufgezeigt werden. Im Abschnitt 4.5 soll eine Zusammenfassung gegeben werden.

4.1 Betrachtung von Fallbeispielen

In diesem Abschnitt soll eine Aufstellung von zwei Fallbeispielen erfolgen, in denen typische Einsatzbereiche von IT-Systemen aufgezeigt werden (vgl. Unterabschnitte 4.1.1 und 4.1.2). Hierbei sollen insbesondere die folgenden Aspekte betrachtet werden:

- Zu welchem Zweck erfolgt der Einsatz des IT-Systems?
- Was sind die Aufgaben der Personen, die das IT-System verwenden?
- Wie kann das IT-System aufgebaut sein?
- Welche Anforderungen werden an das IT-System gestellt?

Des Weiteren sollen im Unterabschnitt 4.1.3 anhand der aufgestellten Fallbeispiele verschiedene Prinzipien der Sicherheit von IT-Systemen aufgezeigt werden, deren Kenntnis z.B. bei der im Abschnitt 4.2 folgenden Erstellung einer Systematik vorausgesetzt wird.

4.1.1 Fallbeispiel 1: Einsatz einer Finanzbuchführung

In diesem Fallbeispiel soll der Einsatz einer Finanzbuchführung betrachtet werden. Grundsätzlich soll mit dem Einsatz einer Finanzbuchführung der im Handelsgesetzbuch (HGB) festgeschriebenen Verpflichtung zur Führung von Büchern nachgekommen werden (vgl. §238 HGB aber auch §141 Abgabenordnung). In der heutigen Zeit wird die Finanzbuchführung im Allgemeinen auf IT-Systemen durchgeführt, wobei oft spezielle Software eingesetzt wird. Hierbei haben die das IT-System verwendenden Personengruppen im Allgemeinen die folgenden Aufgaben zu erfüllen:

- Nutzer:
  Führen die Buchungen, Auswertungen (z.B. Abschlüsse, Bilanz, Kosten- und Leistungsrechnung) und die Revision durch. Diese kann in bestimmten Fällen auch von externen Finanzprüfern durchgeführt werden.

- Management:
  Generell ist davon auszugehen, dass das Management kaum direkten Kontakt mit dem System für die Finanzbuchführung hat. Das Management wird im Allgemeinen keine Buchungen und nur in seltenen Fällen Auswertungen oder Revisionen direkt durchführen. Stattdessen werden oft die (von Nutzern erarbeiteten) Ergebnisse der Auswertungen und der Revision eingesehen.

- Administratoren:
  Sie sind für die Einrichtung, den Betrieb und die Wartung des IT-Systems verantwortlich.

Das in einem derartigen Fall eingesetzte IT-System wird oft als ein Client-Server-System aufgebaut sein, bei dem mehrere Arbeitsplatzrechner (Clients) über ein Rechnernetz mit einem Server verbunden sind, auf dem die Daten zentral vorgehalten werden. Der Zugriff erfolgt dabei im Allgemeinen mit einer speziellen Finanzbuchführungssoftware, die Details des Aufbaus des IT-Systems vor den Nutzern verbirgt.

Generell wird an eine Finanzbuchführung die Anforderung gestellt, dass dabei nach den „Grundsätzen ordnungsmäßiger Buchführung“ (GoB) vorgegangen wird (vgl. §238 HGB). „Die Buchführung muss so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann“ (vgl. §238 HGB). Vorschriften für die Führung der Bücher werden u.a. im §239 HGB gegeben.

Schuppenhauer (vgl. [Sch98]) leitet aus dem Begriff der Ordnungsmäßigkeit in der Buchführung den Begriff der Ordnungsmäßigkeit in der Datenverarbeitung her (vgl. [Ned99, Seite 19]). In diesem Zusammenhang soll einer der dort aufgeführten Grundsätze, die „Ordnungsmäßige Organisation des DV-Bereichs — Grundsatz der Funktionssicherheit“, genauer betrachtet werden. Dieser soll aus folgenden Sicherheitsmerkmalen bestehen (vgl. [Ned99, Seite 19]):

- Verfügbarkeit:
  sichere räumliche Unterbringung, ständige Betriebsbereitschaft, volle Betriebssicherheit
- Risikoabdeckung:
  ausreichender Versicherungsschutz
- Manipulationssicherheit:
  klare personelle Funktionstrennung, Bedienungssicherheit, klare Arbeitsanweisungen
- Datensicherung:
  Datenbeständeschutz (auch im Katastrophenfall), schnelle Rekonstruierbarkeit
- Sicherheitskontrolle:
  Überwachung der Dokumentations-, Kontroll- und Sicherheitsmaßnahmen durch unabhängige Stellen.

4.1.2 Fallbeispiel 2: Softwareentwicklungsabteilung

In diesem Fallbeispiel soll die Entwicklung von Software betrachtet werden. Die beteiligten Personengruppen haben in diesem Fallbeispiel die folgenden Aufgaben zu erfüllen:

- Nutzer:
  In diesem Fall sollen die Entwickler als die Nutzer angesehen werden. Ihre Aufgabe ist es, die zu entwickelnde Software zu spezifizieren, zu implementieren, zu testen und zu warten. Dazu nutzen sie das IT-System. Dabei kann es sowohl Nutzer geben, die alle Aufgaben erfüllen, als auch Spezialisten, die nur einzelne Aufgaben wie z.B. das Testen durchführen.

- Management:
  Als Management können das Management der Organisation, in einem weiteren Sinne aber auch die Leiter der Projekte betrachtet werden. Die Aufgaben des Managements sind vor allem die Personalverwaltung und die Kundenbetreuung. So müssen die Aufgaben auf das Personal verteilt, Konflikte gelöst und die Aufgabenerfüllung überprüft werden. Ferner müssen Aufträge angeworben und Kundenbeziehungen gepflegt werden.

- Administratoren:
  Verantwortlich für die Einrichtung, den Betrieb und die Wartung der IT-Systeme.

Das hier anzunehmende IT-System wird oft als ein Client-Server-System aufgebaut sein, bei dem mehrere Arbeitsplatzrechner (Clients) über ein Rechnernetz mit einem Server verbunden sind, auf dem zentral die aktuelle Version der zu entwickelnden Software vorgehalten wird. Zur Bearbeitung wird auf den Clients eine lokale Kopie erstellt. Die lokal durchgeführten Änderungen werden dann mit der zentralen Version abgeglichen und so auch den anderen Nutzern zugänglich gemacht. Im Allgemeinen werden in einem derartigen Fall Software-Werkzeuge wie Editoren, Compiler und Debugger sowie Software-Werkzeuge zur Versionskontrolle und Planungsunterstützung benötigt.

4.1.3 Auswertung der Fallbeispiele

In diesem Unterabschnitt sollen anhand der betrachteten Fallbeispiele einige Konzepte aufgezeigt und erläutert werden. Bezüglich der Aufgaben der das IT-System verwendenden Personen können in beiden Fallbeispielen Möglichkeiten zur Durchsetzung des Prinzips Pflichtentrennung, des Vier-Augen-Prinzips und des Prinzips der geringsten Privilegien festgestellt werden. Bezüglich des Aufbaus des IT-Systems kann festgestellt werden, dass sich in beiden Fallbeispielen eine Client-Server-Architektur anbietet. Ferner soll das Subjekt-Objekt-Modell betrachtet werden. Im Folgenden sollen diese Prinzipien kurz erläutert und ihre Anwendbarkeit in den Fallbeispielen aufgezeigt werden.

Pflichtentrennung, Vier-Augen-Prinzip und Prinzip der geringsten Privilegien

Die **Pflichtentrennung** (separation of duties) ist ein Mechanismus zur Kontrolle von Missbrauch und Fehlern (vgl. [CW87, Seite 187]). Dabei wird eine umfassende Aufgabe in mehrere Teilaufgaben aufgespalten, die von verschiedenen Personen durchzuführen sind. In beiden Fallbeispielen entsteht eine Pflichtentrennung z.B. dadurch, dass die Aufgaben der Nutzer von den Aufgaben der Administratoren getrennt sind. Im Fallbeispiel 1 kann eine Pflichtentrennung zwischen Personen, die für Buchungen, und Personen, die für die Revision zuständig sind, durchgeführt werden. Im Fallbeispiel 2 kann eine Pflichtentrennung zwischen Personen, die die Software implementieren, und Personen, die sie testen, entstehen. In beiden Fällen werden die von einer Person durchgeführten Handlungen von einer anderen kontrolliert. Man spricht in diesem Zusammenhang auch vom **Vier-Augen-Prinzip** (Four Eyes Principle).

Um Missbrauch durch die Pflichtentrennung vorbeugen zu können, muss außerdem das **Prinzip der geringsten Privilegien** (least privileges) durchgesetzt werden. Dieses Prinzip besagt, dass an eine Person nur die Rechte vergeben werden, die für die Erfüllung ihrer Aufgaben notwendig sind. Im Fallbeispiel 1 erfordert die Durchführung von Buchungen ein Schreibrecht. Bei der Revision ist eine Leserecht ausreichend. Administratoren müssen keine Buchungen o.ä. durchführen können, ein Lese- und Schreibrecht ist daher im Allgemeinen nur im Rahmen der Datensicherung und -wiederherstellung notwendig. Im Fallbeispiel 2 benötigen die Entwickler bzgl. den Quelldateien ein Lese- und Schreibrecht, die Tester bei sog. „Black-Box-Tests“ nur ein Ausführungsrecht und bei sog. „White-Box-Tests“ zusätzlich ein Leserecht. In Bezug auf Leserechte spricht man auch vom **„Need to know“-Prinzip**.

Client-Server-Architektur

In beiden Fallbeispielen kann bezüglich des Aufbaus des IT-Systems angenommen werden, dass im Allgemeinen eine **Client-Server-Architektur** eingesetzt werden würde. Dabei können Dienste eines Servers von den Arbeitsplatzrechnern (Clients) aus genutzt werden (vgl. Abbildung 4.1).

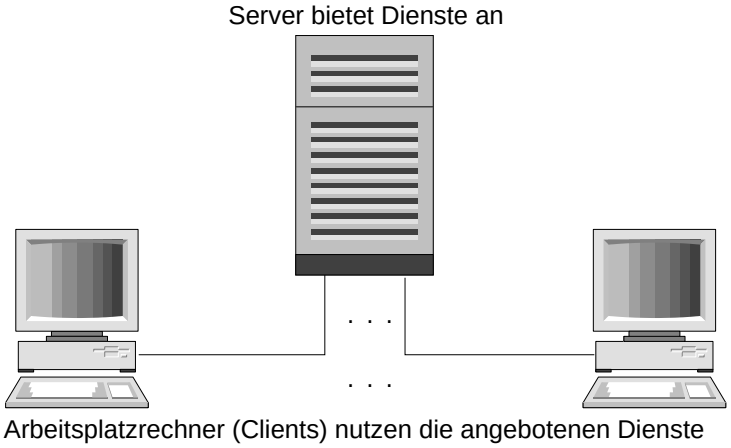


Abbildung 4.1: Client-Server-Architektur

Subjekt-Objekt-Modell

Bezüglich des Aufbaus der IT-Systeme kann allgemeiner auch von einem **Subjekt-Objekt-Modell** (SO-Modell) ausgegangen werden (vgl. [Ker95b, Seite 80ff.]). In einem derartigen SO-Modell führen Subjekte Aktionen aus und greifen dabei auf Objekte zu (vgl. Abbildung 4.2). Das SO-Modell wird oft im Zusammenhang mit Prinzipien zur Durchsetzung von Zugriffsrechten angewendet. Die dabei betrachtete Fragestellung ist, wie festgelegt und durchgesetzt werden kann, dass Subjekte nur autorisierte Aktionen mit Objekten durchführen können.

Abbildung 4.2: Subjekt-Objekt-Modell

Ob Bestandteile eines IT-Systems als Subjekte oder als Objekte betrachtet werden, hängt oft von der Sichtweise in einer bestimmten Situation ab. Unter **Subjekten** kann man die aktiven Instanzen in einem IT-System verstehen, also Personen, die von ihnen initiierten Prozesse oder auch die Hardware. **Objekte** stellen im Allgemeinen schutzbedürftige Werte dar und können in physische und logische Objekte unterschieden werden.

Zu **physischen Objekten** kann die Hardware gezählt werden. Ihr Wert für eine Organisation ergibt sich oft aus einem materiellen Wert. In den Fallbeispielen können hierzu alle Rechner (Server und Clients) inkl. der Ein- und Ausgabegeräte, die Rechnernetze und Peripherie, wie z.B. Drucker, gezählt werden.

Zu den **logischen Objekten** können die Daten (inkl. gespeicherter Software) und Prozesse gezählt werden. Ihr Wert ergibt sich oft aus bei einem Ausfall eintretenden Einbußen und evtl. durch den bei einer Wiederherstellung auftretenden Aufwand. In den Fallbeispielen können zu den Daten die Anwendungssoftware (z.B. die Finanzbuchführungssoftware aus dem Fallbeispiel 1), die Betriebssysteme, Treiber etc. und die durch die Anwendung erzeugten Daten (z.B. Buchungssätze im Fallbeispiel 1 bzw. Quellcode, Testdaten im Fallbeispiel 2) gezählt werden.

In einem weiteren Sinne können auch Personen als Objekte gesehen werden. Personen haben insbesondere im Hinblick auf physische Schäden den höchsten Schutzbedarf. Aber auch für die Organisation, der die Personen angehören, sind sie unverzichtbar, da sie im Allgemeinen das Wissen über die Geschäftsabläufe und die Bedienung der IT-Systeme haben (vgl. [FKB89]). Im Zusammenhang mit Personen werden Gefährdungen wie Feuer u.Ä. betrachtet, die durch Gegenmaßnahmen wie die Installation von Rauchmeldern, Sprinkleranlagen, Ausweisung von Notausgängen u.a. bekämpft werden. Da dies nicht von informatischem Interesse ist, soll dies nicht weiter betrachtet werden. **Aktionen** sind in diesem Zusammenhang Zugriffe wie z.B. ausführen, lesen, schreiben oder die Vergabe von Rechten.

Während der Wert von Objekten in vielen Fällen gemessen werden kann – sehr oft wird hierfür der Aufwand für die Wiederherstellung bzw. einer Ersatzbeschaffung angesetzt – gibt es auch schutzbedürftige **Subjekt-Objekt-Beziehungen** (SO-Beziehungen) in einem IT-System, deren Werte für eine Organisation nicht auf diese Weise abgeschätzt werden können. Trotzdem haben auch diese SO-Beziehungen einen Schutzbedarf. Derartige SO-Beziehungen sind z.B. die Verbindung zwischen einem Client und einem Server (genauer zwischen Prozessen auf Client und Server) aber auch die Beziehung zwischen Personen und Diensten des IT-Systems.

4.2 Erstellung einer Systematik

In diesem Abschnitt soll eine Systematik zur Aufstellung und Einordnung der in diesem Kapitel aufzustellenden Szenarien aufgezeigt werden. Zunächst sollen im Unterabschnitt 4.2.1 die Anforderungen ausgeführt werden, die an die Szenarien gestellt werden sollen. Dann sollen im Unterabschnitt 4.2.2 die Rollen aufgezeigt werden, in denen Nutzer in den Szenarien auftreten können. Um bei der Aufstellung der Szenarien eine notwendige „Breite“ zu erreichen, soll hier angelehnt an das im Unterabschnitt 2.2.4 eingeführte Verfahren zur Erstellung von IT-Sicherheitspolitiken eine Verwundbarkeitsmatrix aus schutzbedürftigen Werten und Schutzzielen eines IT-Systems aufgestellt werden (vgl. Unterabschnitt 4.2.3).

4.2.1 Feststellung von Anforderungen

Mit den hier aufzustellenden Szenarien sollen solche sicherheitsrelevanten Ereignisse aufgezeigt werden, bei denen die Nutzer grundsätzlich einen positiven Beitrag zur Vermeidung oder Bekämpfung dieses Ereignisses leisten können. Das heißt, sie müssen grundsätzlich in der Lage sein, bei vorbeugenden, erkennenden oder korrigierenden Maßnahmen mitwirken zu können (vgl. Unterabschnitt 2.1.3).

- Um bei vorbeugenden Maßnahmen mitwirken zu können, muss es sich um Ereignisse handeln, bei denen Nutzer grundsätzlich in der Lage sind, der betroffenen Verwundbarkeit des IT-Systems entgegenzuwirken. Dies ist z.B. der Fall, wenn Reaktionen der Nutzer ein Bestandteil eines Angriffs sind, die Nutzer also selbst einen wesentlichen Teil der Verwundbarkeit darstellen.

- Um bei entdeckenden Maßnahmen mitwirken zu können, muss es sich um Ereignisse handeln, bei denen Nutzer das Ereignis selbst oder Auswirkungen des Ereignisses beobachten können. Dabei müssen auch Fälle berücksichtigt werden, bei denen die Nutzer das Beobachtete falsch interpretieren (z.B. können nicht den Erwartungen entsprechende Reaktionen des IT-Systems von Nutzern generell als Auswirkung eines Viruses angesehen werden) oder nicht eindeutig als sicherheitsrelevantes Ereignis identifizieren können.

- Korrigierende Maßnahmen befinden sich grundsätzlich nicht in dem im Abschnitt 2.3 abgegrenzten Aufgabenbereich der Nutzer, sondern in dem der Administratoren. Daher sollen sie im Rahmen dieser Arbeit nicht weiter betrachtet werden.

4.2.2 Rollen der Nutzer

In diesem Unterabschnitt sollen die Rollen, die Nutzer bei sicherheitsrelevanten Vorfällen einnehmen können, betrachtet werden. Dabei soll die in Abbildung 4.3 aufgezeigte Unterscheidung vorgenommen werden.

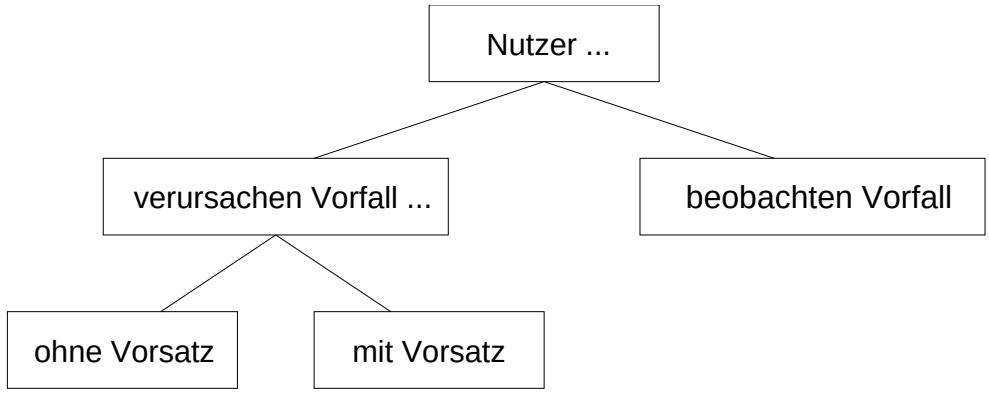


Abbildung 4.3: Unterscheidung der möglichen Rollen der Nutzer bei Vorfällen

Nutzer verursachen sicherheitsrelevante Vorfälle ohne Vorsatz
Unter diesem Punkt sollen die Fälle betrachtet werden, in denen sicherheitsrelevante Vorfälle dadurch entstehen, dass Nutzer Fehler machen. Dabei können grundsätzlich Fehler unterschieden werden, die durch Unkenntnis oder durch Unaufmerksamkeit (so genannte Flüchtigkeitsfehler) entstehen. Oft sind IT-Systeme sehr anfällig gegen derartige Fehler (vgl. Abschnitt 1.1). Aus solchen Fehlern können sich Angriffspunkte ergeben. Diese können unter Umständen auch von einem Angreifer provoziert werden.

Nutzer verursachen sicherheitsrelevante Vorfälle mit Vorsatz
Hier kann weiter zwischen zwei Fällen unterschieden werden:

- Nutzer missachten ihnen bekannte Regelungen oder umgehen Schutzmaßnahmen, die z.B. ihre Arbeitsabläufe erschweren oder auch lediglich abändern (vgl. Unterabschnitt 3.2.2), grundsätzlich handeln sie dabei aber nicht mit der Absicht, der Organisation zu schaden. Oft kann dieses Verhalten auf Unverständnis für den Zweck der Maßnahmen bzw. Regelungen zurückgeführt werden. Auch aus solchem Verhalten können sich Angriffspunkte ergeben.

- Nutzer sind Angreifer. Sie umgehen Regelungen und Schutzmaßnahmen mit Vorsatz, um sich oder anderen einen Vorteil zu verschaffen bzw. der Organisation einen Schaden zuzufügen (vgl. Abschnitt 2.3). Nutzer haben dabei gegenüber externen Angreifern den Vorteil, dass sie grundsätzlich Zutritt zu Gebäuden und einen autorisierten Zugriff auf das IT-System haben. Ferner ist es für sie unter Umständen einfacher, Informationen über Aufbau und Schutzmechanismen des IT-Systems in Erfahrung zu bringen. Der Aufwand für die Durchführung von Angriffen kann daher bei angreifenden Nutzern geringer sein als bei externen Angreifern.

  Nutzer sollen in diesem Zusammenhang bereits dann als Angreifer betrachtet werden, wenn sie einen Missbrauch der Ressourcen des IT-Systems oder einen Diebstahl

begehen. Als Diebstahl soll hier auch das Entwenden von Daten und insbesondere lizenzrechtlich geschützter Software betrachtet werden.

Nutzer werden Zeugen von sicherheitsrelevanten Vorfällen
Hier sollen Fälle betrachtet werden, in denen Nutzer nicht in einem direkten Verhältnis mit der Ursache des sicherheitsrelevanten Vorfalls stehen, sie aber die Möglichkeit haben, Auswirkungen des Vorfalls zu beobachten. Dabei ist zu beachten, dass das Beobachtete von den Nutzern oft nicht eindeutig als ein sicherheitsrelevanter Vorfall erkannt werden kann.

Bezüglich der aufzustellenden Szenarien sollen die Fälle „Nutzer verursachen sicherheitsrelevante Vorfälle ohne Vorsatz“ und “Nutzer verursachen sicherheitsrelevante Vorfälle mit Vorsatz aber ohne Absicht der Organisation zu schaden“ zusammengefasst werden. Dies wird damit begründet, dass in derartigen Fällen oft nicht eindeutig unterschieden werden kann, ob Vorsatz zugrunde lag. Es soll in diesen Fällen angenommen werden, dass die Nutzer eine Verwundbarkeit des IT-Systems darstellen. In den Fällen, in denen Nutzer das IT-System angreifen, sollen sie als Bedrohung und in den Fällen, in denen sie Zeuge von Vorfällen werden, als Beobachter betrachtet werden (vgl. Abbildung 4.4).

<table>
<tr><td colspan="4">Nutzer ...</td></tr>
<tr><td colspan="3">verursachen Vorfall ...</td><td rowspan="2">werden Zeuge von Vorfällen</td></tr>
<tr><td rowspan="2">ohne Vorsatz</td><td colspan="2">mit Vorsatz ...</td></tr>
<tr><td>ohne Schadensabsicht</td><td>mit Schadensabsicht</td><td></td></tr>
<tr><td colspan="2">Nutzer sind Verwundbarkeit</td><td>Nutzer sind Bedrohung</td><td>Nutzer sind Beobachter</td></tr>
</table>

Abbildung 4.4: Nutzer als Verwundbarkeit, Bedrohung und Beobachter

Viele Szenarien können dieser Unterteilung nicht eindeutig zugeordnet werden, da z.B. durch Nutzer verursachte Verwundbarkeiten von angreifenden Nutzern ausgenutzt werden können und der daraus entstehende Vorfall von weiteren Nutzern beobachtet werden kann.

4.2.3 Aufstellung einer Verwundbarkeitsmatrix

In diesem Unterabschnitt soll zunächst aufgezeigt werden, welches die bei der Aufstellung der Verwundbarkeitsmatrix betrachteten schutzbedürftigen Werte und Schutzziele sind. Für die Felder der sich so ergebenen Verwundbarkeitsmatrix sollen dann Beispiele für Verwundbarkeiten aufgezeigt werden.

Bei der Aufstellung der Verwundbarkeitsmatrix sollen die folgenden schutzbedürftigen Werte und Schutzziele berücksichtigt werden (vgl. Tabelle 4.1):

- Schutzziele
  Es sollen die im Unterabschnitt 2.1.3 eingeführten Klassen von Schutzzielen in einem IT-System Vertraulichkeit, Integrität und Verfügbarkeit betrachtet werden.

- schutzbedürftige Werte
  Bei den schutzbedürftigen Werten soll zwischen Objekten und Subjekt-Objekt-Beziehungen unterschieden werde (vgl. Unterabschnitt 4.1.3).

	Objekte	SO-Beziehungen
Vertraulichkeit		
Integrität		
Verfügbarkeit		

Tabelle 4.1: Dimensionen der hier betrachteten Verwundbarkeitsmatrix

Im Folgenden soll für die einzelnen Felder der Verwundbarkeitsmatrix aufgezeigt werden, wie Verwundbarkeiten grundsätzlich aussehen können.

Betrachtung der Objekte

- Vertraulichkeit
  Bezüglich der Vertraulichkeit ist bei den Objekten insbesondere die Vertraulichkeit von Daten relevant. Der Bedarf, Daten vertraulich zu halten, kann aus Interessen der Organisation (z.B. bei Produktionsabläufen oder Strategien) oder aus Gesetzesvorgaben (z.B. bei personenbezogenen Daten) entstehen. Die Vertraulichkeit von Daten kann z.B. dadurch verletzt werden, dass diese bei der Aufbewahrung oder dem Transport nicht hinreichend vor unautorisierten Zugriffen geschützt sind.

  Des Weiteren kann eine Vertraulichkeit bzgl. der eingesetzten Hard- und Software in Bezug auf eine Erschwerung von Angriffen sinnvoll sein. So kann die Kenntnis über die eingesetzte Hard- und Software, insbesondere auch der eingesetzten Versionen, für Angreifer, die spezielle Schwächen ausnutzen wollen, und für Diebe interessant sein. Die Vertraulichkeit bzgl. der eingesetzten Hard- und Software kann z.B. dadurch verletzt werden, dass die Räumlichkeiten, in denen sie eingesetzt wird, betreten bzw. eingesehen werden können oder beim Verbindungsaufbau zwischen IT-Systemen diesbezüglich Informationen ausgetauscht werden.

- Integrität
  Auch bei der Integrität ist insbesondere die Integrität der Daten (im Sinne von gespeicherter Information und Software) zu betrachten. Eine Verletzung der Integrität kann dazu führen, dass Software nicht mehr verfügbar ist oder sie nicht gewünschte Funktionen durchführt bzw. dass gespeicherte Informationen nicht mehr verfügbar sind oder zu falschen Abläufen oder Entscheidungen führen. Die Integrität von Daten kann z.B. dadurch verletzt werden, dass Speicher- oder Übertragungsfehler auftreten oder vorsätzlich Manipulationen durchgeführt werden.

  Eine Verletzung der Integrität der Hardware kann zu einem Verlust der Verfügbarkeit führen. Ferner kann eine Modifikation für Angriffe genutzt werden, wenn z.B. Sicher-

heitsmechanismen manipuliert werden. Eine Verletzung der Integrität von Hardware kann durch Umwelteinflüsse oder durch vorsätzliche Modifikation geschehen.

- Verfügbarkeit
  Die Verfügbarkeit ist bzgl. aller Arten von Objekten relevant. Sind Daten, Hard- oder Software nicht verfügbar, so stellt dies im Allgemeinen eine Beeinträchtigung der mit dem IT-System zu erfüllenden Aufgaben dar. Die Verfügbarkeit kann z.B. dadurch verletzt werden, dass die Integrität verletzt oder Daten gelöscht bzw. Hardware entwendet wird.

Betrachtung der SO-Beziehungen

- Vertraulichkeit
  Bei der Vertraulichkeit von SO-Beziehungen soll die Vertraulichkeit darüber gewahrt werden, auf welche Objekte (z.B. Daten und Dienste) Subjekte zugreifen. Die Vertraulichkeit von SO-Beziehungen kann z.B. dadurch verletzt werden, dass das IT-System Möglichkeiten bietet, Zugriffe und Verbindungen anzeigen zu lassen, oder Verbindungen mitgelesen werden können.

- Integrität
  Bei der Integrität von SO-Beziehungen soll die Authentizität des Subjekts bzw. des Objekts sichergestellt werden. Die Integrität von SO-Beziehungen kann durch eine Maskierung (Masquerading) der Authentizität des Subjekts oder des Objekts verletzt werden. Eine Maskierung eines Subjekts kann z.B. dadurch geschehen, dass ein Angreifer den Zugang eines legitimen Nutzers verwendet. Eine Maskierung eines Objekts kann z.B dann auftreten, wenn es einem Angreifer möglich ist, einen von ihm kontrollierten Rechner so zu konfigurieren, dass dieser sich als ein Server ausgibt und die dadurch getäuschten Nutzer auf diesen zugreifen.

- Verfügbarkeit
  Bei der Verfügbarkeit von SO-Beziehungen soll die Verfügbarkeit des Objekts und die Verfügbarkeit der Verbindung zwischen Subjekt und Objekt gewährleistet werden. Diese Sichtweise soll damit begründet werden, dass die Nichtverfügbarkeit des Objekts bzw. der Verbindung zwar Auswirkungen auf das Subjekt, umgekehrt eine Nichtverfügbarkeit des Subjekts im Allgemeinen keine Auswirkungen auf das Objekt hat. Neben den bereits betrachteten Möglichkeiten der Verletzung der Verfügbarkeit von Objekten gibt es Möglichkeiten, die Verfügbarkeit von Verbindungen zu verletzen, wenn es z.B. möglich ist, diese zu überlasten oder zu unterbrechen.

4.3 Erarbeitung der Szenarien

In diesem Abschnitt sollen die Szenarien aufgestellt werden. Bei der Aufstellung eines Szenarios sollen insbesondere die folgenden Punkte aufgeführt werden:

- Art des sicherheitsrelevanten Ereignisses
  - Welcher schutzbedürftige Wert ist betroffen?
  - Welche Verwundbarkeit ist betroffen?
  - Welche Bedrohung kann das Ereignis auslösen?
- Rolle der Nutzer
- Einordnung in die im vorhergehenden Abschnitt aufgestellte Systematik

Zur besseren Übersicht soll eine Einteilung der Szenarien in Themenbereiche erfolgen. So sollen zunächst verschiedene Szenarien, in denen eine nicht angemessene Verwendung von Passworten erfolgt, betrachtet werden. Dann folgen Szenarien zu den Themenbereichen „Social Engineering"-Techniken, Diebstahl und Missbrauch, beobachtbare Vorfälle und Kommunikationsbeziehungen.

4.3.1 Nicht angemessene Verwendung von Passworten

Oft müssen sich Personen gegenüber einem IT-System als legitime Nutzer authentisieren. Dies erfolgt im Allgemeinen durch eine Identifikation (z.B. durch Namen oder Benutzerkennung) und einer anschließenden Verifikation durch das IT-System aufgrund von Wissen, Besitz, Merkmal oder auch Ort und Zeit. Eine Authentisierung wird durchgeführt, um einer nicht legitimen Nutzung von IT-Systemen entgegenzuwirken oder um durchgeführte Aktionen eindeutig Personen zuordnen zu können. Oft werden zur Authentisierung Passwort-Systeme eingesetzt, bei denen jeder legitime Nutzer eines IT-Systems zur Verifikation ein Passwort verwendet, das keiner anderen Person bekannt sein sollte. Diese Passworte stellen schutzbedürftige Werte dar.

Oft werden die Passworte nicht vorgegeben, sondern von den Nutzern selbst gewählt. Des Weiteren ist es möglich, dass einzelne Personen für verschiedene IT-Systeme oder auch für verschiedene Aufgaben auf einem IT-System mehrere Passworte benötigen. Hieraus können sich verschiedene Probleme ergeben, die in den folgenden Szenarien behandelt werden sollen.

> **Szenario 1: Es werden sehr einfache Passworte benutzt**
> Um sich die Passworte besser merken zu können, werden oft Passworte gewählt, die aus Namen oder regulären Wörtern bestehen. Diese Passworte können von einem Angreifer z.B. durch so genannte Wörterbuchangriffe sehr einfach ermittelt werden. Es kann angenommen werden, dass sehr oft dann „schwache" Passworte gewählt werden, wenn nicht bekannt ist, auf welche Weise Angreifer Passworte ermitteln:
>
> > „I would have thought that if you picked something like your wife's maiden name or something then the chances of a complete stranger guessing *********, in my case, were pretty remote" (vgl. [AS99, Seite 42])

Aus Sicht eines Nutzer handelt es sich um eine Verwundbarkeit bei der Vertraulichkeit von Objekten (Daten), die im Allgemeinen nicht vorsätzlich erzeugt wird.

Szenario 2: Passworte werden aufgeschrieben
Wenn Schwierigkeiten bestehen, sich die Passworte zu merken, z.B. weil Passworte vorgegeben werden, sie sehr häufig geändert werden müssen oder für verschiedene Aufgaben oder IT-Systeme verschiedene Passworte benötigt werden, besteht die Gefahr, dass die Passworte aufgeschrieben und z.B. in der Nähe des Arbeitsplatzes aufbewahrt werden. Aus Sicht eines Nutzer handelt es sich um eine Verwundbarkeit bei der Vertraulichkeit von Objekten (Daten), die in diesem Fall vorsätzlich erzeugt wird.

Szenario 3: Passworte werden mehrfach benutzt
Wenn für verschiedene Aufgaben oder IT-Systeme Passworte benötigt werden, kann der Fall eintreten, dass an verschiedenen Stellen dasselbe Passwort verwendet wird. In so einem Fall muss das Passwort nur an einer Stelle, die z.B. niedrigeren Sicherheitsstandards unterliegt, ermittelt werden und kann dann auch an den anderen Stellen, die u.U. höheren Sicherheitsstandards unterliegen, verwendet werden. Ferner kann der Fall eintreten, dass Passworte mehrfach genutzt werden, wenn bei einem IT-System zwar die regelmäßige Änderung der Passworte gefordert wird, es aber nicht verhindert wird, dass Passworte zyklisch wiederverwendet werden. Aus Sicht eines Nutzer handelt es sich um eine Verwundbarkeit bei der Vertraulichkeit von Objekten (Daten).

Szenario 4: Passworte werden vergessen
Insbesondere nach Wochenenden, nach einem Urlaub oder nach der Änderung von Passworten kommt es vor, dass Passworte vergessen werden. Dies hat zunächst zur Folge, dass Dienste des IT-Systems nicht mehr zur Verfügung stehen. Im Allgemeinen wird in einem derartigen Fall so vorgegangen, dass das Passwort von einem Administrator geändert oder auf einen initialen Wert zurückgesetzt wird. Dies kann durch persönliches Vorsprechen, telefonisch oder auch über Formulare veranlasst werden. In allen Fällen besteht das Problem, dass vom Administrator die Identität der Person festgestellt werden muss, um sicherzustellen, dass eine autorisierte Änderung von Passworten erfolgt.

In diesem Fall tritt ein Verlust der Verfügbarkeit von Objekten und daraus folgend ein Verlust der Verfügbarkeit von SO-Beziehungen auf. Außerdem kann eine Verwundbarkeit bei der Integrität von SO-Beziehungen (Administrator – Nutzer) auftreten.

4.3.2 „Social Engineering“-Techniken

Bei „Social Engineering“-Techniken handelt es sich um nicht-technische Verfahren, bei denen ein Angreifer versucht, gegenüber anderen Personen Autorität oder Vertrauen aufzubauen, um z.B. Informationen zu erlangen oder Personen zu Handlungen zu bewegen. Eine detaillierte Beschreibung verschiedener Techniken des „Social Engineering“ findet sich in [Gor95].

Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet
Hier soll angelehnt an das Beispiel in [Gor95, Seite 448] ein Szenario betrachtet werden, bei dem sich der Angreifer telefonisch mit einem Nutzer in Verbindung setzt und dabei vorgibt ein Administrator zu sein. Dabei soll angenommen werden, dass es das Ziel des Angreifers ist, das Passwort des Nutzers in Erfahrung zu bringen. Dieses Vorgehen funktioniert sehr häufig, da Administratoren von Nutzern oft als wichtige und „allwissende“ Personen angesehen werden, die außerdem gegenüber den Nutzern ein gewisses Machtpotential besitzen. Ferner werden sie oft von Nutzern als Personen wahrgenommen, für die die normalen, für die Nutzer geltenden Regeln oft nicht zutreffen. Daher werden Passworte von Nutzern u.U. sogar bekannt gegeben, wenn ihnen die Regelung bekannt ist, nach der sie ihre Passworte an niemanden weitergeben dürfen (vgl. hierzu auch [Gre96, Seite 14]). Auf diese Weise kann ein Angreifer auch versuchen, Nutzer dazu zu veranlassen, bestimmte Eingaben oder Einstellungen vorzunehmen oder Informationen an den Angreifer weiterzugeben.

Die Nutzer stellen in diesem Szenario eine Verwundbarkeit des IT-Systems dar. Grundsätzlich zeigt dieses Szenario einen Angriff auf die Integrität einer SO-Beziehung auf, bei der die Rolle eines Administrators von einem Angreifer maskiert wird. Das von einem Angreifer eigentlich verfolgte Ziel ist im Allgemeinen aber ein Angriff auf die Vertraulichkeit oder die Integrität von Daten.

Szenario 6: Dateien im Anhang (Attachment) von elektronischen Nachrichten (Emails) werden geöffnet
In diesem Szenario soll angenommen werden, dass Dateien, die Nutzer im Anhang von Emails erhalten, von ihnen geöffnet („angeklickt“) werden. Dies kann sehr oft geschehen, wenn Attachments von ihnen für die Arbeitsabläufe benötigt werden. Es sind aber auch Fälle denkbar, in denen die Attachments nicht für die Arbeitsabläufe benötigt werden, aber trotzdem von den Nutzern geöffnet werden. Dieses Verhalten kann eine Verwundbarkeit darstellen, da es möglich ist, dass Attachments einen Virus oder ein Trojanisches Pferd enthalten. Von Angreifern können verschiedene „Social Engineering“-Techniken eingesetzt werden, um Nutzer dazu zu verleiten ein Attachment anzuklicken. Zunächst wird von Angreifern oft versucht, den Eindruck zu erwecken, dass derartige Emails

von dem Empfänger bekannten Personen abgesandt wurden. Nach den ersten Vorfällen wie z.B. dem Makrovirus „Melissa“ (vgl. [CER99]) wurden viele Personen vorsichtiger und öffneten nicht mehr alle anhängenden Dateien, auch wenn sie scheinbar von bekannten Personen versandt wurden. In der Folge wurde von Angreifern versucht, mit der Namenswahl bei der angehängten Datei den Anreiz zu erhöhen (vgl. z.B. den „Love Letter Worm“ [CER00]) oder den wahren Inhalt zu verschleiern (vgl. z.B. OnTheFly (Anna Kournikova) [CER01]).

Es handelt sich hierbei um einen Angriff auf die Integrität einer SO-Beziehung, z.B. zwischen einem maskierten Sender und einem Nutzer. Unter Umständen sind weitere Schadfunktionen eingebunden, die z.B. einen Angriff auf die Vertraulichkeit bzw. Integrität von Daten oder die Verfügbarkeit von Diensten durchführen sollen.

Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet
Emails, die gefälschte Virus-Warnungen enthalten, werden neben anderen per Email verbreiteten Falschmeldungen als „Hoax“ bezeichnet. Merkmale dieser gefälschten Virus-Warnungen sind unter anderen, dass der vermeintliche Virus als besonders gefährlich oder sogar als „intelligent“ dargestellt wird, dabei meistens auf eine vertrauenswürdige Organisation verwiesen wird und eine besonders eindringliche Aufforderung, die Email an alle bekannten Personen und Adresslisten weiterzuleiten, aufgenommen wird.

Dies stellt einen vorsätzlichen Angriff auf die Integrität einer SO-Beziehung dar (z.B. zwischen dem Sender und Empfänger oder auch zwischen der referenzierten vertrauenswürdigen Organisation und dem Empfänger). Ferner wird die Verfügbarkeit von Nutzern eingeschränkt, da sie für einen gewissen Zeitraum von ihren Pflichten abgehalten werden.

4.3.3 Diebstahl und Missbrauch

Szenario 8: Teile des IT-Systems können entwendet werden
Bei IT-Systemen gibt es viele Bestandteile, die nicht besonders groß oder schwer sind, aber einen sehr großen Wert haben. Ferner haben die in Organisationen eingesetzten IT-Systeme oft eine hohe Kompatibilität untereinander, aber auch zu privat eingesetzten IT-Systemen. Im Zusammenhang mit Daten ist zu beachten, dass von einem Dieb im Allgemeinen eine Kopie entwendet wird, so dass ein Diebstahl in einem derartigen Fall nicht einfach festgestellt werden kann. Aus diesen Gründen kann angenommen werden, dass ein Diebstahl möglich und auch lohnend sein kann. Hierbei müssen sowohl externe als auch interne Personen betrachtet werden. Dies stellt einen Angriff auf die Verfügbarkeit von Objekten (Hardware) bzw. der Vertraulichkeit von Daten dar.

Szenario 9: Missbrauch des IT-Systems für private Zwecke
Dienste, die innerhalb einer Organisation für die Aufgabenerfüllung angeboten werden, können unerlaubt für private Zwecke missbraucht werden. Als Beispiele können hier die Nutzung von Internetzugängen oder private Ausdrucke genannt werden. Dies kann eine Einschränkung der Verfügbarkeit der Ressourcen nach sich ziehen.

Szenario 10: „Salamiangriff“
Unter „Salamiangriff“ wird ein Angriff verstanden, bei dem versucht wird, die einzelnen Schritte so klein zu halten, dass dieser nicht entdeckt wird. Ein berühmtes Beispiel hierfür ist eine persönliche Bereicherung dadurch zu vertuschen, dass ausschließlich äußerst kleine Beträge entwendet werden. Ein derartiger Angriff stellt im Allgemeinen einen Missbrauch der Kompetenzen dar. Dies soll in diesem Zusammenhang als eine Verletzung der Integrität von SO-Beziehungen gewertet werden. Als Folge eines solchen Angriffs kann der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit von Objekten und dabei insbesondere von Daten auftreten.

4.3.4 Beobachtbare Vorfälle

Szenario 11: Dienste stehen nicht mehr zur Verfügung
Ein Dienst ist wider erwarten nicht verfügbar. Dies stellt aus Sicht eines Nutzers eine Verletzung der Verfügbarkeit von SO-Beziehungen dar. In einem derartigen Fall sind Nutzer oft nicht in der Lage, die Ursache hierfür festzustellen. Mögliche Ursachen können sein:

- Der Dienst wurde mit einer sog. „Denial of Service“-Attacke angegriffen.
- Der Dienst ist aufgrund von Fehlern oder Ähnlichem nicht verfügbar.
- Der Dienst ist durch eine zu hohe Anzahl legitimer Nutzer überlastet.
- Der Dienst wurde von Administratoren z.B. für Wartungsarbeiten deaktiviert.

Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus
Es ist möglich, dass ein Angreifer Zugriff auf den Zugang eines Nutzers erlangt hat, indem er z.B. das Passwort ermitteln oder Hintertüren einbauen konnte. Der Angreifer kann diesen Zugang nun missbrauchen, um unter Verwendung der Rechte des Nutzers weitere Angriffe gegen die Organisation oder auch gegen Dritte durchzuführen. Dies würde eine Verletzung der Integrität von SO-Beziehungen darstellen. In so einem Fall ist es möglich, dass dem legitimen Besitzer des Zugangs oder anderen Nutzern Unregelmäßigkeiten auffallen, wie

z.B. dass während der Abwesenheit des Nutzers von diesem Zugang Dienste aufgerufen wurden. Auch in diesem Fall ist es Nutzern aber oft nicht möglich, dies eindeutig festzustellen.

4.3.5 Kommunikationsbeziehungen

Szenario 13: Kommunikationsbeziehungen werden belauscht
Werden Daten ausgetauscht, so besteht grundsätzlich die Möglichkeit, diesen Austausch abzufangen und vom Inhalt Kenntnis zu erlangen. Dies gilt für Kommunikationsbeziehungen zwischen Personen (z.B. Email), zwischen Personen und dem IT-System (z.B. Tastatureingaben oder Bildschirmausgaben), aber auch zwischen IT-Systemen (z.B. Kommunikation zwischen Client- und Server-Systemen). Oft benötigt ein Angreifer dafür Zugriff auf ein IT-System, das sich bezüglich des Weges, auf dem die Daten übertragen werden, zwischen Sender und Empfänger befindet. Man spricht deswegen in diesem Zusammenhang auch von einem „Man in the Middle"-Angriff. Dies stellt einen Angriff auf die Vertraulichkeit von SO-Beziehungen dar. Unter Umständen hat ein Angreifer sogar die Möglichkeit, die übertragenen Daten zu modifizieren, und somit auch die Integrität der SO-Beziehung zu verletzen.

4.4 Einordnung der Szenarien in die Systematik

In diesem Abschnitt soll in zwei Tabellen ein Überblick über die Einordnung der Szenarien in die im Abschnitt 4.2 aufgestellten Systematiken gegeben werden. In der Tabelle 4.2 wird die Einordnung bzgl. der Rollen aufgezeigt, die die Nutzer in den erarbeiteten Szenarien annehmen können. In der Spalte „Nutzer als Angreifer" sind verschiedene Einträge mit Klammern versehen „(x)". Dies soll andeuten, dass die in diesen Szenarien angedeuteten Verwundbarkeiten auch von Nutzern, die Angreifer sind, ausgenutzt werden können.

In der Tabelle 4.3 ist die bei der Aufstellung durchgeführte Zuordnung zu den Feldern der im Unterabschnitt 4.2.3 aufgestellten Verwundbarkeitsmatrix aufgeführt. Dabei kann festgestellt werden, dass in den hier aufgestellten Szenarien für alle Felder der Verwundbarkeitsmatrix Verwundbarkeiten aufgezeigt wurden. Es ist aber zu beachten, dass keine gleichmäßige Verteilung entstanden ist. So wurden z.B. bzgl. der Vertraulichkeit der Objekte in sieben Szenarien bzgl. der Vertraulichkeit von SO-Beziehungen aber nur in einem Szenario Verwundbarkeiten aufgezeigt.

4.5 Zusammenfassung

In diesem Kapitel sollten Szenarien entwickelt werden, die sicherheitsrelevante Vorfälle aufzeigen, an denen Nutzer als Verursacher oder Beobachter beteiligt sind. Dazu wurden zunächst im Abschnitt 4.1 zwei Fallbeispiele für den möglichen Einsatz von IT-Systemen

	Verwundbarkeit	Angreifer	Beobachter
1 Es werden sehr einfache Passworte benutzt	x	(x)	
2 Passworte werden aufgeschrieben	x	(x)	x
3 Passworte werden mehrfach benutzt	x	(x)	
4 Passworte werden vergessen	x		
5 Telefonische Anfragen nach Passworten werden beantwortet	x	(x)	x
6 Dateien im Anhang von Emails werden geöffnet	x	(x)	x
7 Emails mit gefälschten Virus-Warnungen werden weitergeleitet	x	(x)	x
8 Teile des IT-Systems können entwendet werden		x	x
9 Missbrauch des IT-Systems für private Zwecke		x	x
10 „Salamiangriff“		x	x
11 Dienste stehen nicht mehr zur Verfügung		(x)	x
12 Angreifer führt Angriffe vom Zugang eines Nutzers aus	x	(x)	x
13 Kommunikationsbeziehungen werden belauscht		(x)	

Tabelle 4.2: Rollen der Nutzer in den aufgezeigten Szenarien

– „Einsatz einer Finanzbuchführung“ und „Softwareentwicklungsabteilung“ – betrachtet. Anhand dieser Fallbeispiele wurden die folgenden Prinzipien der Sicherheit von IT-Systemen eingeführt: Pflichtentrennung, Vier-Augen-Prinzip und das Prinzip der geringsten Privilegien. Ferner wurden die Client-Server-Architektur und das Subjekt-Objekt-Modell betrachtet.

Im Abschnitt 4.2 wurden zunächst die von den Szenarien zu erfüllenden Anforderungen festgestellt. Hierzu gehört insbesondere das Vorhandensein von Möglichkeiten der Nutzer, einen positiven Beitrag zur Bekämpfung der den Szenarien zugrunde liegenden sicherheitsrelevanten Vorfällen leisten zu können. Es wurde festgestellt, dass dies bei den Nutzern für vorbeugende und entdeckende Maßnahmen, im Allgemeinen aber nicht für korrigierende Maßnahmen gilt. Dem folgend wurden die verschiedenen Rollen aufgezeigt, die Nutzer innerhalb der Szenarien annehmen können. Dabei wurde unterschieden, ob Nutzer den Vorfall ohne oder mit Vorsatz verursachen bzw. ihn beobachten. Bei mit Vorsatz verursachten Vorfällen wurde weiterhin bzgl. einer dem Vorfall zugrunde liegenden Schadensabsicht unterschieden. Als Ergebnis wurde eine Unterscheidung der drei Fälle Nutzer ist Verwundbarkeit, Bedrohung oder Beobachter aufgezeigt. Zum Abschluss des Abschnitts wurden die Dimensionen einer Verwundbarkeitsmatrix bestimmt, die eine notwendige „Breite“ bei der Auswahl der Szenarien veranschaulichen soll. Als Schutzziele wurden Vertraulichkeit, Integrität und Verfügbarkeit, als schutzbedürftige Werte Objekte und SO-Beziehungen angenommen. Für die einzelnen Felder der Verwundbarkeitsmatrix wurde gezeigt, dass grundsätzlich relevante Verwundbarkeiten existieren.

		Objekte			SO-Bezieh.		
		Vertraulichkeit	Integrität	Verfügbarkeit	Vertraulichkeit	Integrität	Verfügbarkeit
1	Es werden sehr einfache Passworte benutzt	x					
2	Passworte werden aufgeschrieben	x					
3	Passworte werden mehrfach benutzt	x					
4	Passworte werden vergessen			x			x
5	Telefonische Anfragen nach Passworten werden beantwortet	x	x			x	
6	Dateien im Anhang von Emails werden geöffnet	x	x	x		x	
7	Emails mit gefälschten Virus-Warnungen werden weitergeleitet			x		x	
8	Teile des IT-Systems können entwendet werden	x		x			
9	Missbrauch des IT-Systems für private Zwecke			x			
10	„Salamiangriff“	x	x	x		x	
11	Dienste stehen nicht mehr zur Verfügung						x
12	Angreifer führt Angriffe vom Zugang eines Nutzers aus					x	
13	Kommunikationsbeziehungen werden belauscht				x	x	

Tabelle 4.3: Zuordnung der Szenarien zu den Feldern der Verwundbarkeitsmatrix

Im Abschnitt 4.3 erfolgte die Aufstellung von dreizehn Szenarien. Dabei wurde eine Einteilung der Szenarien in die folgenden Themenbereiche vorgenommen: Nicht angemessene Verwendung von Passworten, „Social Engineering“-Techniken, Diebstahl und Missbrauch, beobachtbare Vorfälle und Kommunikationsbeziehungen.

Im Abschnitt 4.4 wurde dann die Einordnung der Szenarien in die erstellte Systematik aufgezeigt. Dabei wurde festgestellt, dass alle betrachteten Rollen der Nutzer und Verwundbarkeiten für alle Felder der aufgestellten Verwundbarkeitsmatrix durch die in den aufgestellten Szenarien aufgezeigten Vorfälle abgedeckt werden.

Kapitel 5

Nutzer einbeziehende Schutzmaßnahmen

- Ziel:
  Aufstellung eines Katalogs von Schutzmaßnahmen, bei denen Nutzer aktiv einbezogen werden.
- Vorgehen:
  1. Ermittlung der Unterstützungsmöglichkeiten der Nutzer
  2. Aufstellung der Schutzmaßnahmen

In diesem Kapitel sollen Schutzmaßnahmen aufgezeigt werden, bei denen eine Einbeziehung der Nutzer erfolgt. Grundsätzlich sollen die hier aufgeführten Schutzmaßnahmen gegen die im vorhergehenden Kapitel in den Szenarien aufgezeigten sicherheitsrelevanten Vorfälle gerichtet sein. Eine Gegenüberstellung der in den Szenarien aufgezeigten Verwundbarkeiten zu den Auswirkungen der in diesem Kapitel zu erarbeitenden Schutzmaßnahmen wird im folgenden Kapitel 6 erfolgen.

Zunächst soll im Abschnitt 5.1 aufgezeigt werden, welche Unterstützungsmöglichkeiten durch die Nutzer angenommen werden können. Dann sollen im Abschnitt 5.2 die Schutzmaßnahmen aufgezeigt werden. Abschließend soll im Abschnitt 5.3 eine Zusammenfassung gegeben werden.

5.1 Betrachtung der von Nutzern leistbaren Unterstützungsmöglichkeiten

In diesem Abschnitt soll aufgezeigt werden, welche Möglichkeiten zur Unterstützung von Schutzmaßnahmen die Nutzer grundsätzlich haben. Dazu soll im Unterabschnitt 5.1.1 eine Betrachtung der im Unterabschnitt 2.1.3 eingeführten verschiedenen Arten und Wirkungen von Schutzmaßnahmen erfolgen. Dem folgend sollen im Unterabschnitt 5.1.2 die Auswirkungen auf die Aufgaben und Arbeitsabläufe von Nutzern betrachtet werden. Zum Abschluss dieses Abschnitts soll im Unterabschnitt 5.1.3 betrachtet werden, welche Annahmen einem ausschließlichen Einsatz von Maßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, zugrunde liegen können.

5.1.1 Betrachtung der Arten und Wirkungen von Schutzmaßnahmen

Im Unterabschnitt 2.1.3 wurde zwischen physikalischen, organisatorischen und technischen Schutzmaßnahmen unterschieden. Wie bereits im Abschnitt 1.2 angedeutet, sollen hier aus folgenden Gründen nur organisatorische Maßnahmen betrachtet werden.

- Physikalische Schutzmaßnahmen können von Nutzern im Allgemeinen nicht beeinflusst werden. Es gibt allerdings Bereiche, in denen organisatorische Maßnahmen sehr eng mit physikalischen verbunden sind. Als Beispiel sei hier genannt, dass durch organisatorische Maßnahmen gewährleistet werden muss, dass eine Tür, die als physikalische Schutzmaßnahme gegen unberechtigten Zutritt oder Feuer schützen soll, geschlossen gehalten und nicht z.B. durch ein Stück Pappe blockiert wird.

- Auch technische Maßnahmen sollen laut der im Abschnitt 2.3 durchgeführten Beschreibung der Aufgaben der betrachteten Personengruppen nicht im Bereich der Nutzer liegen. Aber auch hier gibt es sehr enge Verbindungen mit organisatorischen Maßnahmen, wenn z.B. der Umgang mit und die Anwendung von technischen Maßnahmen festgelegt wird.

Ferner wurde im Unterabschnitt 2.1.3 eine Unterscheidung der Wirkung von Schutzmaßnahmen in Vorbeugend, Erkennend und Wiederherstellend durchgeführt. Es wurde bereits im Unterabschnitt 4.2.1 begründet, dass im Zusammenhang mit den Nutzern nur Maßnahmen zur Vorbeugung und Erkennung betrachtet werden sollen.

5.1.2 Auswirkungen auf Aufgaben und Arbeitsabläufe

Bezüglich der Aufgabenbereiche der Nutzer soll festgestellt werden, dass diese grundsätzlich nicht um weitere Aufgaben und insbesondere nicht um Aufgaben aus anderen Bereichen, wie z.B. aus dem Bereich der Administratoren, erweitert werden sollen. Vielmehr sollen die Schutzmaßnahmen lediglich die Arbeitsabläufe in einer Art anpassen, dass zum Schutz

des IT-Systems beigetragen wird. Ferner soll durch die Maßnahmen das Bewusstsein der Nutzer in einer Art geschult werden, dass sie sensibler auf Fragen der Sicherheit von IT-Systemen reagieren.

5.1.3 Annahmen bei Nutzer nicht einbeziehenden Schutzmaßnahmen

Oft wird versucht Sicherheit ausschließlich durch Maßnahmen zu erreichen, bei denen keine Einbeziehung der Nutzer erfolgt. Bei den in solchen Fällen eingesetzten Maßnahmen handelt es sich oft um technische Maßnahmen wie Filtersysteme (z.B. Firewalls), einbruchserkennende Systeme (Intrusion Detection Systeme, IDS), Kontrollen der Passwortwahl und -änderung usw. Einige dieser Maßnahmen werden im Kapitel 7 noch genauer betrachtet werden. Einem derartigen Vorgehen können z.B. die folgenden Annahmen bezüglich der Notwendigkeit bzw. der Auswirkungen einer Einbeziehung von Nutzern zugrunde liegen:

- Das IT-System muss nur gegen Bedrohungen von „Außen“ geschützt werden. Daher werden nur die „Grenzen“ wie Netzübergänge und Zugänge zu Gebäuden geschützt. Dazu ist die Mitwirkung der Nutzer oft nur in Bezug auf die Kooperation bei Zutritts- oder Zugriffskontrollen notwendig.

- Bereits im Abschnitt 1.1 wurde angedeutet, dass Nutzer oft als Sicherheitsproblem (Verwundbarkeit oder Bedrohung) angesehen werden. Um die durch die Nutzer entstehenden Verwundbarkeiten einzuschränken, werden oft technische Maßnahmen eingesetzt, die den „Unzulänglichkeiten“ der Nutzer entgegenwirken sollen. Als Beispiel können hier Passwort-Systeme genannt werden, die u.a. die Auswahl der Passworte und die regelmäßige Änderung von Passworten überprüfen können. Um einer Bedrohung durch die Nutzer entgegenzuwirken, werden an diese oft möglichst wenig Informationen über Sicherheitsmechanismen weitergegeben. Dies soll verhindern, dass diese Informationen von den Nutzern zur Durchführung von Angriffen genutzt werden können (Security by obscurity).

5.2 Aufstellung von Schutzmaßnahmen

In diesem Abschnitt sollen Schutzmaßnahmen aufgezeigt werden, bei denen die Nutzer involviert sind. Diese sollen dann in den folgenden Kapiteln nach verschiedenen Kriterien bewertet werden. Beim Aufzeigen der Schutzmaßnahmen sollen die folgenden Punkte betrachtet werden:

- Es soll das bei der Schutzmaßnahme angewendete Vorgehen skizziert werden.

- Es soll aufgezeigt werden, welche Ziele verfolgt werden.

- Es soll die Rolle der Nutzer besonders hervorgehoben werden.

Zunächst sollen einige Schutzmaßnahmen aufgezeigt werden, die zur Sensibilisierung der Nutzer bzgl. der Fragen der Sicherheit von IT-Systemen beitragen können (vgl. Unterabschnitt 5.2.1). Dann sollen Maßnahmen aufgezeigt werden, die die Arbeitsabläufe der Nutzer bzgl. Aufgaben aus dem Bereich Sicherheit von IT-Systemen ergänzen (vgl. Unterabschnitt 5.2.2).

5.2.1 Maßnahmen zur Sensibilisierung der Nutzer

In vielen Fällen können Nutzer sicherheitsrelevante Vorfälle verschulden, ohne dass sie sich dessen bewusst sind. Dieser Fall wurde im Unterabschnitt 4.2.2 mit „Nutzer ist Verwundbarkeit“ bezeichnet. In derartigen Fällen fehlt sehr oft eine Sensibilisierung der Nutzer für Fragen der Sicherheit der IT-Systeme. Zusätzlich können Nutzer oft auch das Gefühl bekommen, dass sie sich grundsätzlich richtig verhalten. Dies kann u.a. folgende Gründe haben:

- Andere Nutzer verhalten sich genauso.
- Auch das Management als Vorbildrolle verhält sich genauso.
- Es ist seit langer Zeit kein Vorfall eingetreten.
- Aufgrund ihrer Einschätzung gibt es keine Verwundbarkeiten (vgl. hierzu auch **Szenario 1: Es werden sehr einfache Passworte benutzt**).

Ferner ist es möglich, dass Nutzer Angriffe auf das IT-System einer Organisation durchführen, da sie sich nicht bewusst sind, dass ihre Handlungen einen Angriff darstellen, bzw. sie sich nicht bewusst sind, wie groß der Schaden ist, den sie damit verursachen. Um den hieraus entstehenden Vorfällen vorzubeugen, sollten Nutzer bzgl. der Sicherheit von IT-Systemen sensibilisiert werden.

Bekanntmachung der IT-Sicherheitspolitik

Wie bereits im Unterabschnitt 2.2.4 festgestellt, ist es notwendig, für die Bekanntmachung der IT-Sicherheitspolitik Sorge zu tragen. Wird die IT-Sicherheitspolitik nicht auf angemessene Weise bekannt gemacht, so kann dies unbewusste Verstöße bedingt durch mangelnde Kenntnis der einzuhaltenden Vorschriften zur Folge haben. Aus diesen unbewussten Verstößen können Verwundbarkeiten des IT-Systems entstehen. So kann es z.B. sein, dass in der IT-Sicherheitspolitik zwar Anforderungen aufgeführt sind, die bei der Auswahl von Passworten erfüllt werden müssen, Nutzer aber trotzdem einfache Passworte wählen, da ihnen diese Regelungen nicht bekannt sind (vgl. **Szenario 1: Es werden sehr einfache Passworte benutzt**).

Oft reicht es bei der Bekanntmachung der IT-Sicherheitspolitik nicht aus, die Nutzer darüber zu informieren, wo die IT-Sicherheitspolitik eingesehen werden kann, bzw. in einem Umlaufverfahren von allen Nutzern bestätigen zu lassen, dass sie die IT-Sicherheitspolitik gelesen haben. Eine Ursache dafür, dass dieses Vorgehen oft nicht zu einer gewünschten

Sensibilisierung der Nutzer führt, ist, dass die IT-Sicherheitspolitik im Allgemeinen nicht für die Nutzer formuliert wurde. Diese sind u.U. nicht in der Lage zu beurteilen, welche Teile für sie relevant sind und zu welchen Handlungsweisen sie veranlasst werden sollen.

Es sollte in diesem Zusammenhang überlegt werden, im Rahmen einer IT-Sicherheitspolitik einen separaten Teil für die Nutzer zu erstellen, in dem diese Fragen in einer für Nutzer verständlichen Weise behandelt werden, oder Veranstaltungen anzubieten, in denen diese Fragen behandelt werden.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Eine gegen Angriffe, bei denen Nutzer als Verwundbarkeit ausgenutzt werden, gerichtete Schutzmaßnahme ist die Vermittlung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale dieser Angriffe an die Nutzer. Wäre ein derartiges Verständnis bei den Nutzern vorhanden, so würde dies den Nutzern grundsätzlich ermöglichen, derartigen Angriffen vorzubeugen bzw. sie zu erkennen.

Dies kann z.B. in einem Fall eintreten, wie er im **Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet** aufgezeigt wurde. Dadurch dass Nutzer über Ziele und Vorgehensweisen bei Angriffen, die auf „Social Engineering"-Techniken basieren, informiert sind, werden sie im Idealfall in die Lage versetzt, diese besser zu erkennen.

Um ein solches Verständnis bei den Nutzern zu entwickeln, wird es oft notwendig sein, Wissen aus dem Bereich der IT-Systeme und der Sicherheit von IT-Systemen an die Nutzer zu vermitteln. Die Vermittlung des Wissens könnte dabei durch verschiedene Maßnahmen wie Schulungen, Handbücher, regelmäßig erscheinende themenbezogene Informationsblätter o.ä. geschehen.

Vorbeugung von Angriffen durch Nutzer

Unter vorbeugenden Maßnahmen sollen hier solche Maßnahmen verstanden werden, die dazu führen, dass weniger Angriffe von Nutzern durchgeführt werden. Vorbeugende Maßnahmen sollen im Allgemeinen den Aufwand erhöhen, den ein Angreifer aufwenden muss, um einen Angriff durchzuführen. Dabei wird davon ausgegangen, dass ein Angreifer davon abgehalten werden kann, einen Angriff durchzuführen, wenn der dafür notwendige Aufwand im Verhältnis zum Nutzen hinreichend groß ist. Im Zusammenhang mit Angriffen von Nutzern kann eine vorbeugende Maßnahme auch sein, ihnen zu vermitteln, dass sie etwas Verbotenes tun und dass sie dabei einen Schaden anrichten, der sich u.U. auch auf sie (z.B. ihren Arbeitsplatz) auswirken kann.

Gerade beim Missbrauch von Ressourcen der Organisation, wie es im **Szenario 9: Missbrauch des IT-Systems für private Zwecke** angedeutet wurde, können Fälle auftreten, in denen sich Nutzer nicht bewusst sind, dass eine Verwendung für private Zwecke nicht gestattet ist und dadurch für die Organisation unter Umständen ein größerer Schaden entstehen kann, als auf dem ersten Blick ersichtlich ist. Als Beispiel sei hier das Kopieren

von Software oder von urheberrechtlich geschütztem Material genannt. Dies wird oft als ein sog. „Verbrechen ohne Opfer“ gesehen, weshalb die Hemmschwelle hier oft sehr niedrig liegt.

Nutzer werden verantwortlich gemacht

Nutzern kann für die Teile des IT-Systems, die in ihrem Arbeitsbereich liegen, die Verantwortung für bestimmte Aspekte der Sicherheit übertragen werden. Damit kann das Ziel verfolgt werden, die Nutzer dazu zu bewegen, sich mehr für die Sicherheit der IT-Systeme einzusetzen und z.B. auf sie zurückzuführende Verwundbarkeiten einzuschränken. So kann z.B. bezüglich eines Falls, wie er im **Szenario 1: Es werden sehr einfache Passworte benutzt** dargestellt wurde, angenommen werden, dass Nutzer ihre Passworte sorgfältiger auswählen, wenn sie für Verstöße oder Folgen von Verstößen persönlich verantwortlich gemacht werden. Eine Übertragung der Verantwortung kann auch hierarchisch geschehen, wobei Vorgesetzte die Verantwortung für bestimmte Aspekte der Sicherheit der Teile von IT-Systemen haben, die von den ihnen unterstellten Mitarbeitern genutzt werden.

Eine Übertragung der Verantwortung an die Nutzer kann auf verschiedenen Ebenen geschehen:

- Nutzer werden dafür verantwortlich gemacht, dass die gesetzlichen Auflagen wie z.B. Datenschutzgesetze eingehalten werden.
- Nutzer werden für die Einhaltung der IT-Sicherheitspolitik verantwortlich gemacht.
- Nutzer werden dafür verantwortlich gemacht, dass aufgetretene Verwundbarkeiten, Bedrohungen oder Vorfälle sofort gemeldet werden.
- Nutzer werden für einen sicheren Betrieb des IT-Systems verantwortlich gemacht.

Dabei ist grundsätzlich zu klären, welche Konsequenzen bei eingetretenen Vorfällen gezogen werden. Insbesondere wenn Nutzer für einen sicheren Betrieb verantwortlich gemacht werden sollen, ist außerdem zu klären, inwieweit sie Möglichkeiten haben, dies durchzusetzen. Das betrifft einerseits das hierfür notwendige Wissen, andererseits aber auch Möglichkeiten, die Beschaffung und Administration zu beeinflussen. Da diese Möglichkeiten grundsätzlich nicht jedem Nutzer zur Verfügung stehen, wird dieser Grad der Übertragung von Verantwortung im Allgemeinen nur bei Vorgesetzten, wie z.B. Abteilungsleitern, die nicht als Teil des Managements angesehen werden, sinnvoll sein.

5.2.2 Maßnahmen zur Anpassung der Arbeitsabläufe

Durchsetzung der Pflichtentrennung

Das Prinzip der Pflichtentrennung wurde bereits im Unterabschnitt 4.1.3 eingeführt. Dabei wurde festgestellt, dass bei der Pflichtentrennung eine umfassende Aufgabe in mehrere Teilaufgaben aufgespalten wird, die von verschiedenen Personen durchzuführen sind. Dieses

Vorgehen soll es ermöglichen, Fehler zu erkennen. Es wurde ferner festgestellt, dass zur Bekämpfung von Missbrauch auf technischer Ebene das Prinzip der geringsten Privilegien durchgesetzt werden muss. Grundlegend bei diesen Prinzipien ist, dass Nutzer als Beobachter auftreten und die Handlungen von anderen Nutzern bzgl. Fehlern und Missbrauch kontrolliert werden. Dieses Vorgehen kann grundsätzlich gegen einen Angriff wirken, wie er im **Szenario 10: Salamiangriff** dargestellt wurde. Werden die Rechte für die bei einen derartigen Angriff notwendigen Aktionen an verschiedene Personen vergeben, so kann ein Einzelner diesen Angriff grundsätzlich nicht durchführen.

Nutzer melden Sicherheitsvorfälle

Bei dieser Maßnahme soll nicht davon ausgegangen werden, dass Nutzer gezielt nach Vorfällen Ausschau halten. Dies würde nicht in ihren eigentlichen Aufgabenbereich fallen und könnte viele Nutzer auch überfordern. Vielmehr sollen den Nutzern Möglichkeiten aufgezeigt werden, die von ihnen gemachten Beobachtungen, die aus ihrer Sicht sicherheitsrelevant sein können, zur weiteren Überprüfung und eventuellen Einleitung von Gegenmaßnahmen zu melden. Dabei muss betrachtet werden, welche Beobachtungen von Nutzern gemacht werden können und wie weit sie in der Lage sind, diese verlässlich als sicherheitsrelevante Ereignisse zu identifizieren. Hier können starke Wechselwirkungen mit der im Unterabschnitt 5.2.1 aufgestellten Maßnahme „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“ entstehen, da dieses Verständnis auch hier vorteilhaft sein kann.

Ferner muss festgelegt werden, an welche Stellen die Nutzer ihre Beobachtungen melden sollen. Es ist dabei zu überlegen, ob für verschiedene Beobachtungen verschiedene Stellen eingerichtet oder alle Beobachtungen zentral gesammelt werden sollen. Außerdem muss der Fall berücksichtigt werden, in dem die Personen, bei denen die Beobachtungen gemeldet werden, den Missbrauch des IT-Systems selbst durchführen.

Dadurch dass Nutzer ihre Beobachtungen melden, kann z.B. Fällen entgegengewirkt werden, wie sie in den **Szenario 5: Telefonische Anfragen nach Passworten werden beantworte** und im **Szenario 11: Dienste stehen nicht mehr zur Verfügung** aufgezeigt wurden. Im ersten Fall kann eine Meldung derartiger Anrufe genutzt werden, um festzustellen, ob diese Einzelfälle oder einen systematischen Angriff darstellen. Davon abhängig können weitere Maßnahmen wie eine Warnung der Mitarbeiter oder die Überprüfung des IT-Systems veranlasst werden. Im zweiten Fall ist es möglich, dass durch die Meldung der Nutzer der Ausfall schneller bemerkt und in der Folge auch behoben werden kann.

5.3 Zusammenfassung

In diesem Kapitel sollten Schutzmaßnahmen eingeführt werden, bei denen Nutzer involviert sind. Dazu wurden zunächst im Abschnitt 5.1 die von den Nutzern leistbaren Unterstützungsmöglichkeiten betrachtet. Dabei wurde gezeigt, dass ausschließlich organisatorische

Schutzmaßnahmen betrachtet werden sollen, wobei zu beachten ist, dass es organisatorische Schutzmaßnahmen geben kann, die starke Wechselwirkungen mit physikalischen oder technischen Schutzmaßnahmen haben. Es wurde festgestellt, dass die Schutzmaßnahmen so gestaltet sein sollen, dass den Nutzer keine neuen Aufgaben, insbesondere nicht aus dem Aufgabenbereich der Administratoren, zugewiesen werden. Stattdessen soll nur eine Anpassung der Arbeitsabläufe oder eine Sensibilisierung der Nutzer bzgl. der Fragen der Sicherheit von IT-Systemen erfolgen. Zum Abschluss des Abschnitts wurde aufgezeigt, dass einem Einsatz von Maßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, die Annahmen zugrunde liegen können, dass das IT-System nur gegen Bedrohungen von „Außen“ geschützt werden muss oder dass die Nutzer als Verwundbarkeit oder Bedrohung angesehen und daher nicht an Schutzmaßnahmen beteiligt werden.

Im Abschnitt 5.2 erfolgte die Aufstellung der Schutzmaßnahmen. Bei jeder Schutzmaßnahme wurde das Vorgehen, das mit der Maßnahme verfolgte Ziel und die Rolle der Nutzer betrachtet. Es wurde zwischen Maßnahmen unterschieden, mit denen eine Sensibilisierung der Nutzer erreicht werden soll (vgl. Unterabschnitt 5.2.1), und Maßnahmen, die die Arbeitsabläufe der Nutzer anpassen sollen (vgl. Unterabschnitt 5.2.2). Es wurden die folgenden Maßnahmen beschrieben:

- Maßnahmen zur Sensibilisierung der Nutzer
  - Bekanntmachung der IT-Sicherheitspolitik
  - Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen
  - Vorbeugung von Angriffen durch Nutzer
  - Nutzer werden verantwortlich gemacht
- Maßnahmen die Arbeitsabläufe der Nutzer anpassen
  - Durchsetzung der Pflichtentrennung
  - Nutzer melden Sicherheitsvorfälle

Kapitel 6

Eignung und Aufwand-Nutzen-Verhältnis der Schutzmaßnahmen

- Ziel:
  Betrachtung des durch die Schutzmaßnahmen entstehenden Nutzens und Aufwands.
- Vorgehen:
  1. Betrachtung der Wirkungen und des Wirkungsgrades
  2. Betrachtung der durch die Schutzmaßnahmen entstehenden Risiken
  3. Betrachtung des Aufwands bei der Durchsetzung und des Betriebs
  4. Betrachtung des Verhältnisses zwischen Aufwand und Nutzen

In diesem Kapitel soll die Eignung und das Aufwand-Nutzen-Verhältnis der im vorhergehenden Kapitel 5 aufgezeigten Schutzmaßnahmen untersucht werden. Es wurde im Unterabschnitt 2.2.4 gezeigt, dass im Rahmen der Erstellung einer IT-Sicherheitspolitik eine Auswahl und Bewertung von Schutzmaßnahmen erfolgt. Um eine Auswahl von Schutzmaßnahmen zu ermöglichen, sollte für die betrachteten Schutzmaßnahmen ihre Wirkung, ihr Wirkungsgrad, die durch den Einsatz der Maßnahmen entstehenden Risiken und der durch den Einsatz der Maßnahmen entstehende Aufwand bekannt sein.

Bezüglich der Eignung der Schutzmaßnahmen soll im Abschnitt 6.1 betrachtet werden, welche Wirkungen sie auf die im Kapitel 4 aufgezeigten Vorfälle haben können. Ferner sollen im Abschnitt 6.2 die Risiken betrachtet werden, die durch den Einsatz der Schutzmaßnahmen entstehen können. Im Abschnitt 6.3 soll der durch die Maßnahmen entstehende Aufwand betrachtet werden. Im Abschnitt 6.4 soll dann eine Abwägung des Nutzens und des Aufwands der Maßnahmen erfolgen. Schließlich erfolgt im Abschnitt 6.5 eine Zusammenfassung der in diesem Kapitel erarbeiteten Inhalte.

6.1 Betrachtung der Wirkungen und des Wirkungsgrades

In diesem Abschnitt soll betrachtet werden, welche Auswirkungen die im Kapitel 5 aufgezeigten Schutzmaßnahmen auf die in Kapitel 4 in den Szenarien aufgezeigten Vorfälle haben können und in welchem Grad sie den Vorfällen entgegenwirken können. Für eine Organisation, die ein IT-System betreibt, besteht das generelle Ziel dabei darin, die sicherheitsrelevanten Vorfälle einzuschränken. Um dies zu erreichen, sollen generell die Verwundbarkeiten des IT-Systems und Angriffe gegen das IT-System eingeschränkt werden (vgl. Unterabschnitt 2.1.3). Im Zusammenhang mit den hier betrachteten Maßnahmen bedeutet dies, dass Verstößen gegen die IT-Sicherheitspolitik durch Nutzer und den dadurch entstehenden Verwundbarkeiten sowie Angriffen von Nutzern und Externen vorgebeugt bzw. diese erkannt werden sollen (vgl. Unterabschnitt 4.2.1). Daher soll im Folgenden für die einzelnen Schutzmaßnahmen aufgezeigt werden, welchen in den Szenarien aufgezeigten Vorfällen und welchen Ursachen für Vorfälle (beabsichtigte oder unbeabsichtigte Verstöße, Angriffe von Nutzern oder Externen) durch ihren Einsatz entgegengewirkt werden kann.

6.1.1 Maßnahmen zur Sensibilisierung der Nutzer

Bekanntmachung der IT-Sicherheitspolitik

Eine angemessene Bekanntmachung der IT-Sicherheitspolitik soll dazu beitragen, dass durch Nutzer verursachte unbewusste Verstöße gegen in der IT-Sicherheitspolitik festgeschriebene Regeln, die darauf zurückgeführt werden können, dass den Nutzern die Regeln nicht bekannt waren, verringert werden. Derartige unbewusste Verstöße können z.B. in den folgenden Szenarien auftreten:

- **Szenario 1: Es werden sehr einfache Passworte benutzt**,
  Szenario 2: Passworte werden aufgeschrieben
  und **Szenario 3: Passworte werden mehrfach benutzt**
  Es ist denkbar, dass eine nicht angemessene Bekanntmachung der IT-Sicherheitspolitik dazu führt, dass den Nutzern nicht bekannt ist, wie eine im Sinne der IT-Sicherheitspolitik angemessene Verwendung von Passworten zu erfolgen hat. Wählen Nutzer z.B. schwache Passworte aus, so kann dies aus der Sicht der Nutzer ein unbewusster Verstoß gegen die IT-Sicherheitspolitik sein, wenn es den Nutzern aufgrund einer unzureichenden Bekanntmachung der IT-Sicherheitspolitik nicht bekannt ist, dass sie keine schwachen Passworte wählen dürfen. Ferner können Fälle eintreten, in denen Nutzern zwar bekannt ist, dass sie keine schwachen Passworte wählen dürfen, es ist ihnen aber nicht bekannt ist, welche Passworte als schwach einzuschätzen sind. Dies kann u.a. dann eintreten, wenn in der IT-Sicherheitspolitik nicht definiert wurde, was unter schwachen Passworten zu verstehen ist (z.B. da sich dies über die Zeit ändert).

- **Szenario 9: Missbrauch des IT-Systems für private Zwecke**
  Wird den Nutzern nicht in angemessener Weise vermittelt, welche Arten von Nutzung des IT-Systems für private Zwecke gestattet sind und unter welchen Umständen eine private Nutzung erfolgen darf, so können hier nicht beabsichtigte Verstöße entstehen. Selbst im trivialen Fall, in dem die Nutzung für private Zwecke generell nicht gestattet ist, muss beachtet werden, dass die Grenzen aus Sicht der Nutzer nicht immer eindeutig bestimmt werden können. Als Beispiel sei hier eine Nutzung genannt, bei der auch die Fertigkeiten im Umgang mit dem Computer geschult werden, und argumentiert werden kann, dass diese auch der Organisation zugute kommen würden.

  Auch bei den Umständen für eine private Nutzung können Unklarheiten zu unbewussten Verstößen führen. Wird z.B. festgelegt, dass eine private Nutzung nur erfolgen darf, wenn der reguläre Betrieb nicht beeinträchtigt wird, muss hinterfragt werden, inwieweit Nutzer überhaupt Möglichkeiten haben dies festzustellen.

Wurde den Nutzern der für sie relevante Teil der IT-Sicherheitspolitik auf für sie verständliche Weise vermittelt, so kann grundsätzlich davon ausgegangen werden, dass dadurch unbewusste Verstöße stark eingeschränkt werden. Aus der Sicht der das IT-System betreibenden Organisation ist es wichtig, derartige unbewusste Verstöße gegen die IT-Sicherheitspolitik so weit wie möglich zu begrenzen, um die aus diesen Verstößen entstehenden Verwundbarkeiten zu verringern. Für die Nutzer kann die Durchführung dieser Maßnahme den Vorteil haben, dass es für sie bei der Arbeit mit dem IT-System weniger Situationen gibt, in denen sie unsicher sind, welches Verhalten von ihnen erwartet wird.

Keine Wirkung zeigt diese Maßnahme im Allgemeinen gegen Verstöße, die von Nutzern bewusst begangen werden. Dies ist unabhängig davon, ob es sich um einen Angriff durch einen Nutzer handelt oder ob Nutzer ohne Angriffsabsicht gegen Regeln der IT-Sicherheitspolitik verstoßen. Ferner wirkt diese Maßnahme grundsätzlich nicht gegen von Externen durchgeführte Angriffe.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Kennen die Nutzer die Hintergründe und Ziele von Angriffen und sind sie mit Vorgehensweisen von Angreifern und Erkennungsmerkmalen von Angriffen vertraut, so kann davon ausgegangen werden, dass dadurch Verwundbarkeiten, die von ihnen ausgehen, verringert werden. Dies soll durch die Betrachtung der folgenden Szenarien veranschaulicht werden:

- **Szenario 1: Es werden sehr einfache Passworte benutzt**
  Bereits bei der Aufstellung des Szenarios im Kapitel 4 wurde darauf hingewiesen, dass Nutzer oft nicht wissen, wie Passworte von Angreifern ermittelt werden, und sie sich daher nicht bewusst sind, dass sie von einem Angreifer leicht zu ermittelnde Passworte verwenden. Wird den Nutzern vermittelt auf welche Weise solche Angriffe durchgeführt werden und welche Passworte daher als schwach einzuschätzen sind, kann das zur Folge haben, dass weniger schwache Passworte gewählt werden.

- **Szenario 3: Passworte werden mehrfach benutzt**
  Eine mehrfache Verwendung von Passworten wird von Nutzern oft durchgeführt, um die Anzahl der verwendeten und damit zu merkenden Passworte einzuschränken. Dabei ist den Nutzern u.U. nicht bewusst, dass der Schutz der Passworte vor einer nicht autorisierten Kenntnisnahme bei IT-Systemen mit unterschiedlichem Schutzbedarf verschieden hoch sein kann und dass dieser Umstand evtl. von Angreifern ausgenutzt wird. Diese können das Passwort bei IT-Systemen mit geringem Schutz ermitteln und es dann verwenden, um Zugriff auf einem IT-System mit hohem Schutz zu erlangen. Würde dies von den Nutzern verstanden, könnte davon ausgegangen werden, dass diese ihr Verhalten diesem Umstand anpassen und eine mehrfache Verwendung von Passworten unterlassen.

- **Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet**
  In diesem Fall muss von den Nutzern die von potentiellen Angreifern verfolgte Taktik verstanden werden. Voraussetzung ist hierbei, dass den Nutzern bekannt ist, dass sie ihr Passwort unter keinen Umständen bekannt geben dürfen. Darüber hinaus müssen sie verstehen, dass ein Angreifer versuchen wird, sie dazu zu bringen, diese Regelung zu verletzen, indem er z.B. einen Notfall vorgibt und dabei versucht, gegenüber dem Nutzer Sympathie oder Druck aufzubauen. Insbesondere muss gewährleistet und den Nutzern bekannt sein, dass ihnen unter keinen Umständen Nachteile entstehen, wenn sie ihr Passwort nicht am Telefon bekannt geben. Die Durchsetzung dieser Voraussetzung ist außerordentlich wichtig. Gibt es Ausnahmen, in denen Nutzer ihr Passwort am Telefon hätten bekannt geben sollen, so kann dies die Nutzer so sehr verunsichern, dass sie bei einem entsprechend hartnäckigen Angreifer diese Regel u.U. verletzen.

- **Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet**
  In diesem Fall muss den Nutzern klar gemacht werden, dass seriöse Unternehmen derartige Warnungen nicht unaufgefordert per Email versenden. Sie müssen verstehen, dass die oft auftretende eindringliche Aufforderung, diese Email unbedingt an alle Bekannten weiterzuleiten, eine „Social Engineering“-Technik ist, die ihnen gegenüber Druck erzeugen soll.

Werden den Nutzern die Hintergründe, Ziele und Erkennungsmerkmale von Angriffen und die Vorgehensweisen von Angreifern vermittelt, so können dadurch sowohl unbewusste Verstöße als auch bewusste Verstöße ohne Angriffsabsicht und damit die hieraus entstehenden Verwundbarkeiten eingeschränkt werden. Auch diese Maßnahme zeigt keine direkte Wirkung gegen Angriffe von Nutzern oder Externen.

Vorbeugung von Angriffen durch Nutzer

Zur Vorbeugung von Angriffen durch Nutzer sollen diese über Wirkung und Folgen ihres Handelns aufgeklärt werden. Dabei soll ihnen klar gemacht werden, welche Handlungen verboten sind und welche Auswirkungen diese z.B. für die Organisation haben.

- **Szenario 8: Teile des IT-Systems können entwendet werden**
  In Bezug auf den Diebstahl von Hardware kann nicht angenommen werden, dass die Durchführung dieser Maßnahme zu einer Verringerung derartiger Vorfälle führen wird. Im Allgemeinen sind sich Personen bewusst, welchen Wert die Hardware hat und welches die Folgen für die Organisation sind. Wie bereits im Kapitel 4 angedeutet, ist es aber denkbar, dass eine Aufklärung bzgl. der Folgen des Kopierens von Daten und Software dafür sorgen könnte, dass derartige Vorfälle eingeschränkt werden.

- **Szenario 9: Missbrauch des IT-Systems für private Zwecke**
  Auch beim Missbrauch des IT-Systems für private Zwecke ist es denkbar, dass Nutzern oft nicht bewusst ist, welche Folgen dies für die Organisation haben kann. Wird dieses Bewusstsein vermittelt, kann Missbrauch u.U. eingeschränkt werden.

Mit der hier betrachteten Maßnahme sollen gezielt durch Nutzer durchgeführte Angriffe eingeschränkt werden. Dabei kann diese Maßnahme nicht gegen solche durch Nutzer durchgeführte Angriffe wirken, bei denen diese die Absicht haben, durch ihr Handeln der Organisation vorsätzlich Schaden zuzufügen (z.B. aus Rache, vgl. Abschnitt 2.3).

Nutzer werden verantwortlich gemacht

Dadurch dass Nutzer für die Sicherheit der IT-Systeme verantwortlich gemacht werden, soll ihnen gegenüber Druck aufgebaut werden, sich mit der Sicherheit der IT-Systeme zu befassen. Es soll ihnen bewusst gemacht werden, dass sie persönlich zur Rechenschaft gezogen werden, wenn auf sie zurückzuführende Verwundbarkeiten entdeckt werden oder daraus resultierende Vorfälle auftreten.

- **Szenario 1: Es werden sehr einfache Passworte benutzt**
  Die von Angreifern verwendeten Werkzeuge zur Ermittlung von Passworten können natürlich auch von Administratoren genutzt werden, um schwache Passworte zu ermitteln. Wird bei Nutzern festgestellt, dass sie schwache Passworte verwenden, so können sie dafür zur Rechenschaft gezogen werden.

- **Szenario 2: Passworte werden aufgeschrieben**
  Werden die aufgeschriebenen Passworte so gelagert, dass sie von jedem eingesehen werden können, so kann dies ohne Weiteres festgestellt und der Nutzer dafür zur Rechenschaft gezogen werden.

- **Szenario 3: Passworte werden mehrfach benutzt**
  Eine mehrfache Verwendung kann im Allgemeinen nur innerhalb der IT-Systeme einer Organisation festgestellt werden. Dies ist z.B. der Fall, wenn ein zusätzliches Passwort für Dienste eines Servers benötigt wird oder Nutzer für verschiedene Funktionen verschiedene Passworte verwenden sollen.

Dadurch dass Nutzer verantwortlich gemacht werden, wird im Allgemeinen eine abschreckende Wirkung erzielt. Dies kann dazu führen, dass Verwundbarkeiten eingeschränkt werden, die durch bewusste Verstöße gegen die Sicherheitspolitik durch die Nutzer entstehen.

Gegen unbewusste Verstöße kann nur in soweit eine Wirkung erzielt werden, als dass Nutzer sich u.U. genauer mit der IT-Sicherheitspolitik und den von ihnen geforderten Verhalten auseinander setzen. Angriffen von Externen wird dies im Allgemeinen nicht entgegenwirken.

6.1.2 Maßnahmen zur Anpassung der Arbeitsabläufe

Durchsetzung der Pflichtentrennung

Mit der Durchsetzung von Pflichtentrennung und dem Prinzip der geringsten Privilegien soll allgemein Fehlern und Missbrauch entgegengewirkt werden. Im Zusammenhang mit den hier betrachteten Szenarien kann mit der Durchsetzung dieser Prinzipien insbesondere einem Missbrauch von IT-Systemen vorgebeugt werden.

- **Szenario 10: „Salamiangriff“**
  Bei einem „Salamiangriff“ handelt es sich im Allgemeinen um einen Missbrauch. Mit der Durchsetzung der Pflichtentrennung kann grundsätzlich erreicht werden, dass kein Nutzer mehr in der Lage ist, einen solchen Angriff alleine durchzuführen.

- **Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus**
  In einem derartigen Fall könnte es einem Angreifer aufgrund der durchgesetzten Pflichtentrennung nicht möglich sein, den beabsichtigten Angriff durchzuführen, wenn er nur Zugriff auf den Account eines Nutzers und damit auch nur die Rechte eines einzigen Nutzers hat.

Mit der Durchsetzung der Pflichtentrennung kann grundsätzlich sowohl Missbrauch (Angriffe von Nutzern und Externen) als auch Fehlern (Verstöße ohne Schadensabsicht) entgegengewirkt werden. Die Wirkung dieser Maßnahme ist dabei sehr von der Art der Durchsetzung der Prinzipien abhängig. Angriffe oder Verstöße, deren Durchführung nur die Rechte eines Nutzers voraussetzen, können auch bei der Durchsetzung dieser Prinzipien auftreten. Dies gilt z.B. für die Szenarien aus den Bereichen der nicht angemessenen Verwendung von Passworten und den „Social Engineering“-Techniken.

Nutzer melden Sicherheitsvorfälle

Dadurch dass Nutzer die bei der Ausführung ihrer Aufgaben gemachten Beobachtungen melden, denen sicherheitsrelevante Vorfälle zugrunde liegen können, soll eine bessere und frühzeitigere Erkennung von Vorfällen erreicht werden.

- **Szenario 2: Passworte werden aufgeschrieben**
  Werden Passworte aufgeschrieben und offen am Arbeitsplatz hinterlegt, so kann dies von anderen Nutzern beobachtet werden.

- **Szenario 4: Passworte werden vergessen**
  Wie bereits angedeutet muss ein Nutzer, der ein Passwort vergessen hat, dies melden, um durch Maßnahmen wie das Setzen eines neuen oder das Rücksetzen auf ein Standardpasswort wieder Zugriff zu erlangen.

- **Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet** und **Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet**
  Erhält ein Nutzer einen Anruf, in dem er nach seinem Passwort gefragt wird, oder eine Email, die eine gefälschte Virus-Warnung enthält, so sollte dies von ihm gemeldet werden, damit andere Nutzer gewarnt und evtl. Gegenmaßnahmen eingeleitet werden können.

- **Szenario 8: Teile des IT-Systems können entwendet werden** und **Szenario 9: Missbrauch des IT-Systems für private Zwecke**
  Für den Fall, dass Diebstahl oder Missbrauch durch Nutzer beobachtet wird, sollte festgelegt sein, wie in solchen Fällen zu verfahren ist. Ziel sollte es sein, dies zu unterbinden und die Verursacher zur Rechenschaft zu ziehen.

- **Szenario 11: Dienste stehen nicht mehr zur Verfügung**
  Oft sind die Nutzer die Ersten, die feststellen, dass Dienste nicht mehr zur Verfügung stehen. Wenn hier eine sinnvolle Möglichkeit gefunden wird, dies zu melden, kann unter Umständen früher mit der Suche nach der Ursache und mit der Wiederherstellung der Verfügbarkeit des Dienstes begonnen werden.

Diese Maßnahme kann sowohl beabsichtige Verstöße z.B. auch durch externe Angreifer, aber auch unbewusste Verstöße einschränken. Wesentlich hierbei ist, ob die Verstöße durch Nutzer beobachtet werden können.

6.1.3 Einordnung der Wirkungen der Schutzmaßnahmen

In der Tabelle 6.1 wird in einer Übersicht aufgezeigt, gegen welche der in den Szenarien aufgezeigten Vorfälle die aufgeführten Schutzmaßnahmen wirken können. Obwohl durch die Übersicht kein Anspruch auf Vollständigkeit bzgl. der Wirkungen der Schutzmaßnahmen auf Vorfälle erhoben wird, sollen im Folgenden einige Tendenzen festgestellt werden.

- Durch die „Meldung von Vorfällen“ kann vielen der in den Szenarien vorgestellten Vorfällen entgegengewirkt werden. Dabei kann insbesondere festgestellt werden, dass sich die Wirkung dieser Maßnahme über viele der in Kapitel 4 aufgezeigten Themenbereiche erstreckt.

- Durch die Maßnahmen „Bekanntmachung der IT-Sicherheitspolitik“ und “Entwicklung eines Verständnisses“[1] kann mehreren Vorfällen aus verschiedenen Themenbereichen entgegengewirkt werden.

- Durch die Pflichtentrennung kann wenigen Vorfällen aus verschiedenen Themenbereichen entgegengewirkt werden.

[1] Im Rahmen der Auswertung in Tabellen verwendete Kurzform für die Maßnahme „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“

	1	2	3	4	5	6	7	8	9	10	11	12	13
	Maßnahmen zur Sensibilisierung der Nutzer												
Bekanntmachung der Sicherheitspolitik	x	x	x						x				
Entwicklung eines Verständnisses	x		x		x		x						
Vorbeugung von Angriffen durch Nutzer								x	x				
Nutzer werden verantwortlich gemacht	x	x	x										
	Maßnahmen zur Anpassung der Arbeitsabläufe												
Durchsetzung der Pflichtentrennung										x		x	
Nutzer melden Sicherheitsvorfälle		x		x	x		x	x	x		x		

Szenario 1: Es werden sehr einfache Passworte benutzt
Szenario 2: Passworte werden aufgeschrieben
Szenario 3: Passworte werden mehrfach benutzt
Szenario 4: Passworte werden vergessen
Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet
Szenario 6: Dateien im Anhang von Emails werden geöffnet
Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet
Szenario 8: Teile des IT-Systems können entwendet werden
Szenario 9: Missbrauch des IT-Systems für private Zwecke
Szenario 10: „Salamiangriff“
Szenario 11: Dienste stehen nicht mehr zur Verfügung
Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus
Szenario 13: Kommunikationsbeziehungen werden belauscht

Tabelle 6.1: Gegenüberstellung der Szenarien und Schutzmaßnahmen

- Durch die Maßnahmen „Vorbeugung von Angriffen durch Nutzer“ und „Nutzer werden verantwortlich gemacht“ kann jeweils wenigen Vorfällen entgegengewirkt werden, die in denselben Themenbereichen liegen.

- Keine der hier betrachteten Maßnahmen wirkt dem Belauschen von Kommunikationsbeziehungen entgegen.

In der Tabelle 6.2 wird aufgezeigt, gegen welche Ursachen von sicherheitsrelevanten Vorfällen die Schutzmaßnahmen wirken. Dabei kann folgendes festgestellt werden:

- Die Maßnahmen zur Anpassung der Arbeitsabläufe zeigen generell Wirkung gegen alle der hier betrachteten Ursachen. Wie bereits im Unterabschnitt 6.1.2 aufgezeigt, muss aber beachtet werden, dass beide Maßnahmen grundsätzliche Einschränkungen haben. Demnach spielt bei der Pflichtentrennung die Durchsetzung eine wichtige Rolle, während bei der Maßnahme „Nutzer melden Sicherheitsvorfälle“ nur solchen Verstößen entgegengewirkt werden kann, die von Nutzern beobachtet werden können.

- Die Maßnahmen „Entwicklung eines Verständnisses“ und „Verantwortung der Nutzer“ wirken gegen zwei Ursachen, und zwar die durch Nutzer unbewusst oder bewusst herbeigeführten Verstöße, aber nicht direkt gegen von Nutzern oder Externen durchgeführte Angriffe.

	Durch Nutzer verursachte			Externe sind Angreifer
	unbewusste Verstöße	bewusste Verstöße	Angriffe	
	Maßnahmen zur Sensibilisierung der Nutzer			
Bekanntmachung der Sicherheitspolitik	x			
Entwicklung eines Verständnisses	x	x		
Vorbeugung von Angriffen durch Nutzer			x	
Nutzer werden verantwortlich gemacht	x	x		
	Maßnahmen zur Anpassung der Arbeitsabläufe			
Durchsetzung der Pflichtentrennung	x	x	x	x
Nutzer melden Sicherheitsvorfälle	x	x	x	x

Tabelle 6.2: Gegenüberstellung der Schutzmaßnahmen und Ursachen der Verstöße

- Schließlich kann festgestellt werden, dass die Maßnahmen „Bekanntmachung der IT-Sicherheitspolitik“ und „Vorbeugung von Angriffen durch Nutzer“ nur gegen jeweils eine Ursache für Vorfälle Wirkung zeigen.

In der Tabelle 6.3 wird die Gegenüberstellung der Schutzmaßnahmen mit den Szenarien und den Ursachen der Verstöße zusammengefasst. Dabei drücken die Zahlen aus, wie vielen der betrachteten dreizehn Szenarien, fünf Themenbereichen und vier Ursachen für Verstöße durch die Schutzmaßnahmen entgegengewirkt wird. Werden diese Zahlen isoliert, also außerhalb eines bei der Erstellung einer IT-Sicherheitspolitik zu verfolgendem Gesamtkonzeptes betrachtet, so kann festgestellt werden, dass die Maßnahme „Nutzer melden Sicherheitsvorfälle“ die breiteste Wirkung zeigt, gefolgt von den Maßnahmen „Durchsetzung der Pflichtentrennung“, „Entwicklung eines Verständnisses“ und „Bekanntmachung der IT-Sicherheitspolitik“. Die Maßnahmen „Nutzer werden verantwortlich gemacht“ und “Vorbeugung von Angriffen durch Nutzer“ zeigen eine weniger breite Wirkung. Bei der Maßnahme „Vorbeugung von Angriffen durch Nutzer“ kann dies aber insbesondere auf die sehr spezialisierte Ausrichtung der Maßnahme zurückgeführt werden.

	Szenarien (13)	Bereiche (5)	Ursachen (4)
	Maßnahmen zur Sensibilisierung der Nutzer		
Bekanntmachung der Sicherheitspolitik	4	2	1
Entwicklung eines Verständnisses	4	2	2
Vorbeugung von Angriffen durch Nutzer	2	1	1
Nutzer werden verantwortlich gemacht	2	1	2
	Maßnahmen zur Anpassung der Arbeitsabläufe		
Durchsetzung der Pflichtentrennung	2	2	4
Nutzer melden Sicherheitsvorfälle	7	4	4

Tabelle 6.3: Zusammenfassung der Gegenüberstellungen der Schutzmaßnahmen

6.2 Betrachtung des verbleibenden Restrisikos

In diesem Abschnitt sollen die Risiken betrachtet werden, die trotz des Einsatzes der Maßnahmen bestehen bleiben bzw. gerade durch den Einsatz der Maßnahmen entstehen können. Dazu soll zunächst betrachtet werden, unter welchen Umständen die Maßnahmen evtl. nicht im erwarteten Umfang gegen die Verwundbarkeiten wirken (vgl. Unterabschnitt 6.2.1). Dann sollen Möglichkeiten und mögliche Ursachen für die Umgehung der Maßnahmen durch die Nutzer betrachtet werden (vgl. Unterabschnitt 6.2.2). Abschließend sollen Seiteneffekte aufgezeigt werden, die den Nutzen der Maßnahmen einschränken können (vgl. Unterabschnitt 6.2.3).

6.2.1 Mögliche Ursachen für eine eingeschränkte Wirksamkeit

Eine eingeschränkte Wirksamkeit von Schutzmaßnahmen kann auftreten, wenn die Umsetzung der Maßnahmen, also die Implementierung oder die Durchsetzung, in nicht angemessener Weise erfolgt. In diesem Unterabschnitt soll für die hier betrachteten Maßnahmen aufgezeigt werden, welche Ursachen es für eine nicht angemessene Umsetzung geben kann.

Bekanntmachung der IT-Sicherheitspolitik

Wie bereits angedeutet, kann bei dieser Maßnahme eine eingeschränkte Wirksamkeit auftreten, wenn die IT-Sicherheitspolitik unvollständige, unverständliche oder unrealistische Teile enthält, die von den Nutzern nicht nachvollzogen werden können. Ferner kann durch neue Nutzer, denen die IT-Sicherheitspolitik noch nicht bekannt ist, durch Änderungen, die noch nicht angemessen bekannt gemacht worden sind, oder dadurch, dass Nutzer einzelne Aspekte vergessen, eine Einschränkung der Wirksamkeit entstehen.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Bei dieser Maßnahme kann die Wirksamkeit eingeschränkt werden, wenn sich die Entwicklung des Verständnisses nicht an den Bedürfnissen der Nutzer ausrichtet oder die Inhalte für die Nutzer unverständlich aufbereitet sind.

Vorbeugung von Angriffen durch Nutzer

Grundsätzlich ist anzunehmen, dass es sehr schwierig ist, die Nutzer davon zu überzeugen, dass das Kopieren von Daten oder Software Schäden verursacht. Gelingt es nicht, die Nutzer zu überzeugen, so schränkt dies die Wirksamkeit dieser Maßnahme stark ein.

Nutzer werden verantwortlich gemacht

Bereits bei der Aufstellung dieser Maßnahme wurde darauf hingewiesen, dass Probleme auftreten können, wenn die Nutzer keinen Einfluss auf die Ursachen für evtl. auftreten-

de Vorfälle haben, für die sie dann verantwortlich gemacht werden. Ferner wird bei den Nutzern oft nicht das notwendige Wissen vorhanden sein, um eine umfassende Sicherheit verantworten zu können. Zeit oder Möglichkeiten sich dieses Wissen anzueignen, wird den Nutzern oft ebenfalls nicht zur Verfügung stehen.

Durchsetzung der Pflichtentrennung

Bei dieser Maßnahme können mehrere Probleme auftreten, die die Wirksamkeit einschränken können. Zunächst ist es zur Bekämpfung von Missbrauch unbedingt notwendig, das Prinzip der geringsten Privilegien technisch zu implementieren. Wird dies nicht durchgesetzt, können Angriffe von Nutzern weiterhin durchgeführt werden. Auch wenn das Prinzip der geringsten Privilegien durchgesetzt wurde, können immer noch solche Verstöße durchgeführt werden, für die nur die Rechte eines einzelnen Nutzers benötigt werden. Schließlich ist es möglich, dass sich mehrere Nutzer für einen Verstoß zusammentun oder Nutzer von Angreifern z.B. durch „Social Engineering"-Techniken dazu gebracht werden, ihre Rechte im Sinne des Angreifers zu nutzen.

Nutzer melden Sicherheitsvorfälle

Unter Umständen haben Nutzer nicht das notwendige Wissen, um die von ihnen gemachten Beobachtungen richtig einschätzen zu können. Dies kann dazu führen, dass sie zu viel, zu wenig oder falsches melden. Es können auch Probleme auftreten, wenn nicht klar geregelt ist, an welche Stellen die Beobachtungen gemeldet werden sollen. Dies kann im schlimmsten Fall dazu führen, dass sich keine von mehreren möglichen Stellen für zuständig erklärt.

Fazit

Bezüglich der Wirksamkeit der hier betrachteten Maßnahmen kann festgestellt werden, dass eine nicht angemessene Durchsetzung die Wirksamkeit stark einschränken kann. Für eine ein IT-System betreibende Organisation ist eine auf diese Weise eingeschränkte Wirksamkeit aus den folgenden Gründen von Nachteil. Zunächst besteht nicht der Grad an Schutz, der bei der Erstellung der IT-Sicherheitspolitik angenommen wurde. Dies ist insbesondere dann kritisch, wenn dies den Verantwortlichen nicht bewusst ist und daher ein nicht gerechtfertigtes Vertrauen in die Sicherheit des IT-Systems besteht. Ferner beeinträchtigt die durch die nicht angemessene Durchsetzung entstehende eingeschränkte Wirksamkeit das Aufwand-Nutzen-Verhältnis der Maßnahmen, wenn von der Annahme ausgegangen wird, dass die Kosten nicht wesentlich durch die Unterschiede in der Durchsetzung beeinflusst werden.

6.2.2 Möglichkeiten und Ursachen der Umgehung der Maßnahmen durch die Nutzer

Insbesondere wenn von den Nutzern in den Maßnahmen kein Nutzen für die eigenen Arbeitsabläufe gesehen wird, diese aber eine Behinderung oder auch nur eine Änderung

der bekannten Arbeitsabläufe nach sich ziehen, werden sie oft umgangen (vgl. Unterabschnitt 3.2.2). Hier soll näher betrachtet werden, welche Ursachen und Möglichkeiten der Umgehung bei den im vorhergehenden Kapitel 5 aufgezeigten Maßnahmen bestehen.

Bekanntmachung der IT-Sicherheitspolitik

Bei dieser Maßnahme kann angenommen werden, dass die Nutzer grundsätzlich keinen Nutzen für die Erfüllung ihrer Aufgaben sehen. Daher ist zu erwarten, dass sie sich bei den entsprechenden Maßnahmen zur Bekanntmachung der IT-Sicherheitspolitik nicht voll einbringen werden und im Extremfall versuchen nicht an den Maßnahmen teilzunehmen.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Auch bei dieser Maßnahme werden Nutzer im Allgemeinen keinen Nutzen für die Erfüllung ihrer Aufgaben erkennen. Zusätzlich besteht das Problem, dass sie u.U. den Eindruck gewinnen können, dass sich das hierfür notwendige Wissen häufig in einer aus ihrer Sicht grundlegenden Weise ändert. Als Beispiel sei hier aufgeführt, dass Passworte, die nach bestimmten Regeln ermittelt werden, für einen Zeitpunkt als hinreichend sicher gelten können, ein paar Monate oder Jahre später aber als durch einen Angreifer einfach ermittelbar. Besteht dieser Eindruck bei den Nutzern, so kann angenommen werden, dass auch dies dazu beitragen wird, dass ihre Motivation, sich bei den Maßnahmen zur Durchsetzung zu beteiligen, sinken wird.

Vorbeugung von Angriffen durch Nutzer

Auch in diesem Fall ist davon auszugehen, dass die Nutzer keinen Nutzen für die Erfüllung ihrer Aufgaben sehen. Die Bereitschaft an Maßnahmen zur Durchsetzung teilzunehmen und sich überzeugen zu lassen, wird dadurch im Allgemeinen auch hier sinken. Insbesondere in Bezug auf das Kopieren von Software, dass in der Gesellschaft oft als „Kavaliersdelikt“ angesehen wird, muss angenommen werden, dass dies auch beim Einsatz der hier betrachteten Maßnahme praktiziert werden wird, wenn die Nutzer die Möglichkeiten dafür haben und z.B. einen persönlichen Nutzen sehen.

Nutzer werden verantwortlich gemacht

Es kann angenommen werden, dass Nutzer nicht in jedem Fall versuchen werden, den bestmöglichen Grad an Schutz für den Bereich, für den sie verantwortlich sind, zu erlangen. Unter Umständen werden sie lediglich versuchen, einen Grad an Schutz zu erreichen, der besser ist als der von anderen Bereichen. Diesem Vorgehen kann die Hoffnung der Nutzer zugrunde liegen, dass beim Eintreten eines Vorfalls zunächst nicht der eigene, sondern andere, weniger geschützte Bereiche betroffen sind oder ein so großer Bereich betroffen ist, dass sie nicht persönlich zur Rechenschaft gezogen werden.

Durchsetzung der Pflichtentrennung

Aus der Sicht der Nutzer kann die Durchsetzung der Pflichtentrennung dazu führen, dass Arbeitsabläufe aufwendiger werden. Ferner können Probleme auftreten, wenn Personen, die bestimmte Rechte haben, durch Urlaub, Krankheit oder auch nur durch Pausen nicht verfügbar sind, wenn sie bestimmte Aktionen durchführen sollen. Es kann grundsätzlich angenommen werden, dass Nutzer versuchen diese Probleme zu umgehen, indem sie z.B. ihre Passworte anderen Nutzern mitteilen, so dass diese die Möglichkeit haben, mit ihren Rechten Aktionen durchzuführen. Dieses Verhalten würde das Prinzip der Pflichtentrennung aushebeln. Fehler und Missbrauch wären wieder möglich.

Nutzer melden Sicherheitsvorfälle

Grundsätzlich hat die Meldung von Beobachtungen für die Nutzer zur Folge, dass sie die Erfüllung ihrer Aufgaben unterbrechen müssen und dadurch Einbußen in ihrer Produktivität entstehen. Ferner kann das Problem bestehen, dass Nutzer Vorfälle beobachten, die durch ihnen bekannte Personen verursacht werden und diese Vorfälle daher nicht melden, da es nicht üblich ist, Kollegen zu „verpfeifen“. Des Weiteren ist denkbar, dass ein Nutzer selbst einen Vorfall verschuldet hat oder sich vielleicht auch nur nicht sicher ist, ob der beobachtete Vorfall selbst verschuldet ist. In beiden Fällen ist es denkbar, dass Nutzer ihre Beobachtungen aus Furcht vor für sie negativen Konsequenzen nicht melden.

Fazit

Für die Ursachen der Umgehung der Maßnahmen durch Nutzer kann festgestellt werden, dass eine Umgehung zu erwarten ist, wenn die Nutzer in den Maßnahmen keinen Nutzen für sich sehen. Eine Umgehung der Maßnahmen durch die Nutzer kann aber zur Folge haben, dass die Verwundbarkeiten, denen durch die Maßnahmen entgegengewirkt werden sollte, weiterhin bestehen oder sogar weitere, zusätzliche Verwundbarkeiten entstehen. Um dies zu verhindern, ist es notwendig, die Nutzer zu überzeugen, dass der Schutz der Daten und Arbeitsabläufe und damit die Durchführung der Maßnahmen in ihrem eigenen Interesse liegt, um die Organisation und damit ihre Arbeitsplätze zu erhalten. Möglichkeiten hierfür werden im Abschnitt 8.1 betrachtet werden.

6.2.3 Durch die Schutzmaßnahmen bedingte Seiteneffekte

In diesem Unterabschnitt sollen Seiteneffekte aufgezeigt werden, die der Einsatz der Schutzmaßnahmen nach sich ziehen kann. Unter Seiteneffekten sollen dabei solche Folgen des Einsatzes der Schutzmaßnahmen verstanden werden, die neue, unter Umständen ganz andere Sicherheitsprobleme oder auch Auswirkungen im Bereich des Verhältnisses der Nutzer zur Organisation bzw. der Nutzer untereinander nach sich ziehen können.

Bekanntmachung der IT-Sicherheitspolitik

Bei dieser Maßnahme wird den Nutzern ein detailliertes Wissen über die eingesetzten Sicherheitsmaßnahmen vermittelt. Dieses Wissen kann von ihnen grundsätzlich bei der Durchführung von Angriffen genutzt oder an Angreifer weitergegeben werden.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Unter anderem würde den Nutzern bei dieser Maßnahme detailliertes Wissen über das Vorgehen bei Angriffen vermittelt werden. Grundsätzlich können sie auch dieses Wissen nutzen, um selbst Angriffe durchzuführen.

Vorbeugung von Angriffen durch Nutzer

Grundsätzlich entsteht bei dieser Maßnahme das Problem, dass sich die Nutzer pauschal als potentielle Angreifer verurteilt fühlen können, was zu einem gestörten Verhältnis zur Organisation führen kann. Ferner ist es im Rahmen dieser Maßnahme möglich, dass den Nutzern ein genaues Bild darüber vermittelt wird, an welchen Stellen ein Angriff der Organisation wirklich Schaden kann. Zum Beispiel bei Angriffen, die das Ziel haben, sich an der Organisation zu rächen, kann dieses Wissen dann von den Nutzern ausgenutzt werden.

Nutzer werden verantwortlich gemacht

Bei dieser Maßnahme ist es leicht möglich, die Nutzer zu überfordern und bei ihnen damit Unzufriedenheit oder Frustration hervorzurufen. Unter Umständen kann auch Konkurrenzdenken zwischen den Nutzern entstehen, wobei von ihnen versucht wird, einen etwas höheren Grad an Sicherheit als andere zu erlangen, in der Hoffnung, dass diese und nicht sie von eintretenden Vorfällen betroffen sind. Einzelne Nutzer, die besonders erfahren sind, können von anderen Nutzern zu ihren Problemen befragt werden. Außer dass dies die Produktivität dieser Nutzer stark einschränken kann, ist denkbar, dass ein Konkurrenzverhältnis zu den Administratoren aufgebaut wird.

Durchsetzung der Pflichtentrennung

Wurde diese Maßnahme durchgesetzt, so sind u.U. einzelne Personen oder Personengruppen in der Lage Arbeitsabläufe hinauszuzögern. Diese Möglichkeit könnte dazu führen, dass eine Machtstruktur innerhalb der Organisation aufgebaut wird.

Nutzer melden Sicherheitsvorfälle

Es ist denkbar, dass Unstimmigkeiten zwischen Nutzern, die z.B. privater Natur sein können, dazu führen, dass diese die Möglichkeit Beobachtungen zu melden missbrauchen, um Meldungen über den jeweils anderen zu erstellen, mit dem Ziel diesem dadurch zu schaden.

Fazit

In Bezug auf die durch die Schutzmaßnahmen evtl. entstehenden Seiteneffekte kann festgestellt werden, dass sie grundsätzlich negative Auswirkungen auf die Sicherheit des IT-Systems haben können, wenn z.B. die Nutzer in die Lage versetzt werden, Angriffe durchzuführen. Ferner können sie negative Auswirkungen auf eine existierende Organisationskultur haben, wenn das Verhältnis zwischen Nutzern und Organisation oder das Verhältnis zwischen den Nutzern durch den Einsatz der Schutzmaßnahmen negativ beeinflusst wird. Das Ziel muss es hier sein, evtl. auftretende Seiteneffekte zu erkennen, zu bewerten und diejenigen einzuschränken, die negative Auswirkungen in einem nicht vertretbaren Maß nach sich ziehen würden.

6.3 Betrachtung des durch die Maßnahmen entstehenden Aufwands

In diesem Abschnitt soll der Aufwand betrachtet werden, der durch den Einsatz der Schutzmaßnahmen entstehen kann. Dabei soll unterschieden werden in den Aufwand, der durch die Durchsetzung, durch die Wartung und durch den Betrieb der Schutzmaßnahmen entsteht. Unter Aufwand der Durchsetzung soll dabei der durch Implementierung, Bekanntmachung und Motivierung verursachte Aufwand verstanden werden. Unter Aufwand der Wartung soll der Aufwand verstanden werden, der durch die Auffrischung der bei der Bekanntmachung vermittelten Sachverhalte, durch die Erhaltung der Motivation der Nutzer oder durch eine Anpassung der Schutzmaßnahmen an geänderte Bedingungen entsteht. Unter Aufwand des Betriebs soll der für die Nutzer zusätzlich entstehende Aufwand bei der Erfüllung ihrer Aufgaben betrachtet werden.

Bekanntmachung der IT-Sicherheitspolitik

Im Rahmen der Durchsetzung dieser Maßnahme muss die IT-Sicherheitspolitik allen Nutzern bekannt gemacht werden. Dabei ist zu beachten, dass es im Allgemeinen notwendig sein wird, die Nutzer zunächst zu motivieren (vgl. Unterabschnitt 6.2.2). Die Bekanntmachung kann dann z.B. durch Schulungen oder für die Nutzer verfasste Dokumente geschehen.

Zunächst erzeugt die Vorbereitung dieser Schulungen bzw. Dokumente einen Aufwand. Ferner entsteht Aufwand durch die Motivierung der Nutzer und durch die Durchführung der Bekanntmachung. Beim Aufwand, der durch die Durchführung der Motivierung und der Bekanntmachung entsteht, ist insbesondere zu beachten, dass nicht nur Aufwand für die Personen entsteht, die für die Durchführung verantwortlich sind, sondern auch für alle Personen, die mit diesen Maßnahmen erreicht werden sollen. Der für die Durchsetzung dieser Maßnahme anzunehmende Aufwand kann sehr davon abhängen, wie viele Aspekte der IT-Sicherheitspolitik auf die Nutzer zutreffen und wie komplex diese sind. Eine aus wenigen und für die Nutzer unmittelbar verständlichen Regeln bestehende IT-Sicherheitspolitik dürfte weit weniger Aufwand bei der Bekanntmachung erfordern als eine sehr umfassen-

de und mit vielen Spezialfällen behaftete IT-Sicherheitspolitik. Da bei der Durchsetzung dieser Maßnahme sehr viele Personen einbezogen werden müssen, soll der Aufwand für die Durchsetzung hier generell als hoch angenommen werden,

Unter Wartung kann hier u.a. die Bekanntmachung von Änderungen der IT-Sicherheitspolitik und die Bekanntmachung der IT-Sicherheitspolitik bei neuen Nutzern verstanden werden. Insbesondere müssen aber auch bereits bekannt gemachte Aspekte der IT-Sicherheitspolitik periodisch wiederholt werden, um zu verhindern, dass diese über die Zeit vergessen werden. Hierfür soll generell ein mittlerer Aufwand angenommen werden.

Im Rahmen des Betriebs sollte durch diese Maßnahme grundsätzlich kein zusätzlicher Aufwand im Verhältnis zu dem durch die IT-Sicherheitspolitik festgelegten Verhalten entstehen. Es ist allerdings zu beachten, dass für die Nutzer dann ein zusätzlicher Aufwand entstehen kann, wenn sie nach der Bekanntmachung ihre Arbeitsabläufe an ihnen bisher nicht bekannte Regeln anpassen müssen und diese Anpassungen die Arbeitsabläufe aufwendiger gestalten. Generell soll für den Betrieb ein geringer Aufwand angenommen werden.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Auch bei dieser Maßnahme wird es bei der Durchsetzung zunächst wichtig sein, die Nutzer zu motivieren. Die Entwicklung des Verständnisses kann dann ebenfalls z.B. durch Schulungen oder für die Nutzer verfasste Dokumente geschehen. Grundsätzlich kann angenommen werden, dass diese Maßnahme einen höheren Aufwand erfordert als die Bekanntmachung der IT-Sicherheitspolitik. Bei der Bekanntmachung der IT-Sicherheitspolitik sollen den Nutzern lediglich Regeln vermittelt werden, die sie im Zweifelsfall einfach nachschlagen können und die im Idealfall einfach zu verstehen sind. In diesem Fall sollen die Nutzer verstehen, welche Ziele Angreifer haben und wie sie dabei vorgehen. Ferner sollen ihnen Erkennungsmerkmale von Angriffen vermittelt werden. Dabei handelt es sich oft um komplexe und teilweise auch sehr technische Sachverhalte, die von Nutzern u.U. nicht ohne Weiteres verstanden werden können.

Auch bei dieser Maßnahme kann unter Wartung die Behandlung von Änderungen im zu vermittelnden Wissen und die Einweisung von neuen Nutzern verstanden werden. Ferner sollten auch bei dieser Maßnahme Wiederholungen bereits behandelter Aspekte durchgeführt werden. Generell soll von einem mittleren Aufwand für die Wartung ausgegangen werden. Beim Betrieb wird wiederum ein geringer Aufwand angenommen.

Vorbeugung von Angriffen durch Nutzer

In diesem Fall wird bei der Durchsetzung im Allgemeinen versucht, durch Schulungen oder Dokumente die Einstellung von Nutzern zu beeinflussen. Dabei ist das zu betrachtende Themengebiet recht begrenzt. Eine erfolgreiche Überzeugung der Nutzer kann aber als schwierig und daher als mit einem hohen Aufwand verbunden betrachtet werden. Im Rahmen einer Wartung wird wiederum ein mittlerer Aufwand durch die Behandlung von neu hinzukommenden Nutzern angenommen.

Nutzer werden verantwortlich gemacht

Grundsätzlich wird es bei der Durchsetzung dieser Maßnahme nicht ausreichen, die Nutzer davon in Kenntnis zu setzen, dass sie verantwortlich gemacht werden, und festzulegen, mit welchen Konsequenzen Verstöße geahndet werden. Vielmehr muss festgestellt werden, inwieweit die Voraussetzungen für die Nutzer die Verantwortung zu übernehmen gegeben sind. Gegebenenfalls sind diese zu schaffen. Unter anderem in Abhängigkeit vom Grad der Verantwortung, die von den Nutzern übernommen werden soll, müssen diese z.B. geschult oder ihnen Möglichkeiten gegeben werden, die Administration und Beschaffung von IT-Systemen beeinflussen zu können. Damit ist der Aufwand für die Durchsetzung auch abhängig vom Grad der Verantwortung. Generell soll hier von einem hohen Aufwand ausgegangen werden.

Im Rahmen einer Wartung muss insbesondere der aus Änderungen bzgl. der zu übernehmenden Verantwortung und durch neue Mitarbeiter entstehende Aufwand betrachtet werden. Beim Betrieb entsteht ein hoher Aufwand, wenn an die Nutzer ein hoher Grad an Verantwortung übertragen wird und diese daher Zeit zur Absicherung der Systeme benötigen.

Durchsetzung der Pflichtentrennung

Im Rahmen der Durchsetzung hat die organisatorische und technische Umsetzung der Pflichtentrennung und des Prinzips der geringsten Privilegien zu geschehen. Hierbei soll generell ein hoher Aufwand angenommen werden. Eine organisatorische Umsetzung ist notwendig, da die Arbeitsabläufe u.U. nicht in einer Weise ausgelegt sind, dass eine Pflichtentrennung sinnvoll durchgeführt werden kann. Diese müssen in einer sinnvollen Weise abgeändert werden. Die Möglichkeiten einer Durchsetzung hängen dabei auch von den zur Verfügung stehenden personellen Ressourcen ab. So kann in kleinen Organisationen mit nur wenigen Nutzern eine Pflichtentrennung u.U. nicht in einem wünschenswerten Maß umgesetzt werden, da einzelne Personen viele verschiedene Aufgaben zu erfüllen haben. Eine auf technischer Ebene zu erfolgende Durchsetzung des Prinzips der geringsten Privilegien ist wie bereits mehrfach erwähnt notwendig, damit Missbrauch entgegengewirkt werden kann.

Bezüglich der Wartung soll hier ein geringer Aufwand angenommen werden. Dies soll insbesondere damit begründet werden, dass hierbei nur wenige Personen, im Allgemeinen lediglich die Administratoren, einbezogen sind. Im Rahmen des Betriebs ist mit einem zusätzlichen Aufwand zu rechnen, der z.B. dadurch entstehen kann, dass zusätzliche Personen bei der Erfüllung einer Aufgabe einbezogen werden müssen, um eine angemessene Pflichtentrennung gewährleisten zu können.

Nutzer melden Sicherheitsvorfälle

Im Rahmen einer Durchsetzung müssen zunächst die Voraussetzungen geschaffen werden. So müssen z.B. Stellen eingerichtet werden, die Meldungen annehmen, oder Anweisungen gegeben werden, auf welche Weise die Meldungen bearbeitet werden. Des Weiteren muss

eine Einweisung der Nutzer erfolgen. Dabei muss ihnen vermittelt werden, an welche Stellen sie welche Arten von Beobachtungen melden sollen. Der Aufwand hierfür kann generell als hoch angesehen werden. Im Rahmen der Wartung dieser Maßnahme soll ein mittlerer Aufwand angenommen werden, da hier neben evtl. Anpassungen des Verfahrens eine Einweisung von neuen Nutzern notwendig ist. Beim Betrieb dieser Maßnahme entsteht Aufwand dadurch, dass die Nutzer Meldungen verfassen und übermitteln und diese Meldungen bearbeitet werden müssen. Da dies grundsätzlich sehr viele Personen betrifft, soll dieser Aufwand generell als hoch eingeschätzt werden.

Fazit

In Tabelle 6.4 wurde für die Durchsetzung, die Wartung und den Betrieb der hier betrachteten Maßnahmen nach hohen, mittleren und geringen Aufwand unterschieden. Dabei kann

	Durchsetzung	Wartung	Betrieb
	Maßnahmen zur Sensibilisierung der Nutzer		
Bekanntmachung der Sicherheitspolitik	hoch	mittel	gering
Entwicklung eines Verständnisses	hoch	mittel	gering
Vorbeugung von Angriffen durch Nutzer	hoch	mittel	gering
Nutzer werden verantwortlich gemacht	hoch	mittel	gering bis hoch
	Maßnahmen zur Anpassung der Arbeitsabläufe		
Durchsetzung der Pflichtentrennung	hoch	gering	hoch
Nutzer melden Sicherheitsvorfälle	hoch	mittel	hoch

Tabelle 6.4: Übersicht über den durch die Schutzmaßnahmen entstehenden Aufwand

festgestellt werden, dass bei den „Maßnahmen zur Sensibilisierung der Nutzer“ im Allgemeinen ein hoher Aufwand für die Durchsetzung erforderlich sein wird, der u.a. durch eine notwendige Motivierung aller betroffener Nutzer für die Durchführung der Maßnahmen entsteht. Bei der Wartung kann ein als mittel einzuschätzender Aufwand angenommen werden, der insbesondere durch die Einbeziehung neuer Nutzer oder Anpassung an Änderungen begründet werden kann. Beim Betrieb dieser Maßnahmen kann im Allgemeinen ein geringer Aufwand angenommen werden. Als Ausnahme kann hier die Maßnahme „Verantwortung der Nutzer“ angenommen werden, bei der dann ein höherer Aufwand auftritt, wenn der Grad der Verantwortung, den die Nutzer übernehmen müssen, höher ist.

Bei den „Maßnahmen zur Anpassung der Arbeitsabläufe“ ist anzunehmen, dass bei der Durchsetzung ein hoher Aufwand durch die Schaffung der organisatorischen Voraussetzungen entsteht. Bezüglich der Wartung dieser Maßnahmen kann angenommen werden, dass sie aus der Sicht der Nutzer nur einen geringen bis mittleren Aufwand nach sich ziehen. Beim Betrieb dagegen kann angenommen werden, dass durch die Anpassung der Arbeitsabläufe ein hoher Aufwand entsteht.

6.4 Betrachtung des Verhältnisses des Aufwands zum Nutzen

In diesem Abschnitt soll eine Betrachtung des Verhältnisses des Nutzens der Maßnahmen zu dem durch die Maßnahmen entstehenden Aufwand durchgeführt werden. Dazu soll zunächst im Unterabschnitt 6.4.1 aufgezeigt werden, wie dieses Verhältnis im Allgemeinen zu ermitteln ist. Dann sollen im Unterabschnitt 6.4.2 diesbezüglich einige Betrachtungen zu den im Kapitel 5 aufgezeigten Schutzmaßnahmen erfolgen und anschließend im Unterabschnitt 6.4.3 einige Aussagen zu einem kombinierten Einsatz dieser Schutzmaßnahmen gemacht werden.

6.4.1 Allgemeine Betrachtung zur Ermittlung von Aufwand und Nutzen von Schutzmaßnahmen

Unter dem **Nutzen einer Schutzmaßnahme** können die Kosten für Ausfall und Wiederherstellung verstanden werden, die durch den Einsatz der Maßnahme vermieden werden können. Unter dem **Aufwand einer Schutzmaßnahme** wären die Kosten zu verstehen, die durch den Einsatz der Schutzmaßnahme entstehen würden (z.B. durch Anschaffung, Einrichtung, Betrieb und Wartung). Dabei ist eine quantitative Messung (vgl. Unterabschnitt 2.2.4) dieser Größen oft nicht einfach möglich. Um z.B. die durch den Einsatz einer Schutzmaßnahme eingesparten Kosten zu ermitteln, wäre es notwendig, festzustellen welche Vorfälle aufgrund des Einsatzes der Maßnahme nicht aufgetreten sind und welche Kosten beim Auftreten der Vorfälle entstanden wären. Beides kann im Allgemeinen nicht bestimmt, sondern im besten Fall z.B. aufgrund von Erfahrungswerten lediglich abgeschätzt werden. Noch schwieriger wird die Bestimmung, wenn ein Vorfall nur durch einen kombinierten Einsatz mehrerer Maßnahmen verhindert werden konnte und die dadurch eingesparten Kosten z.B. anteilig aufgeteilt werden sollen. Auch bei den durch die Schutzmaßnahmen entstehenden Kosten können Probleme bei der Bestimmung auftreten, wenn z.B. übergreifende Kostenpositionen auf die verschiedenen Maßnahmen aufgeteilt werden sollen. Bei der folgenden Betrachtung der im Kapitel 5 aufgezeigten Maßnahmen kann ferner nicht von einem quantitativen Vergleich der Kosten ausgegangen werden, da zu ihrer Ermittlung grundsätzlich ein konkretes Einsatzszenario notwendig wäre und die Kosten in unterschiedlichen Szenarien verschieden ausfallen würden. Daher soll hier ein eher qualitativer Vergleich der Maßnahmen erfolgen.

6.4.2 Betrachtung des Verhältnisses von Aufwand und Nutzen für die einzelnen Maßnahmen

In diesem Unterabschnitt sollen die einzelnen Schutzmaßnahmen bzgl. des von ihnen erzeugten Verhältnisses von Aufwand zu Nutzen betrachtet werden. Dabei wird davon ausgegangen, dass der Nutzen einer Maßnahme durch ihre im Abschnitt 6.1 diskutierte Wirkung, eingeschränkt durch evtl. auftretende Risiken (vgl. Abschnitt 6.2), bestimmt wird.

Der durch die Maßnahme entstehende Aufwand wurde durch die im Abschnitt 6.3 durchgeführten Betrachtungen über den Aufwand bei der Durchsetzung, Wartung und dem Betrieb der Maßnahme aufgezeigt.

Bekanntmachung der IT-Sicherheitspolitik

Es konnte gezeigt werden, dass diese Maßnahme grundsätzlich einen relativ eingeschränkten Nutzen hat, da sie generell nur zur Vorbeugung gegen Verwundbarkeiten eingesetzt werden kann, die auf unbewusste Verstöße gegen Regeln der IT-Sicherheitspolitik basieren. Wie bei allen hier betrachteten Maßnahmen zur Sensibilisierung der Nutzer, kann von einem hohen Aufwand bei der Durchsetzung dieser Maßnahme ausgegangen werden, der auf die Einbeziehung aller Nutzer bei der Durchführung der Motivierung und der Bekanntmachung zurückgeführt werden kann. Im Gegensatz dazu erzeugt diese Maßnahme nur sehr geringen bis gar keinen Aufwand beim Betrieb, beeinflusst also kaum die normalen Arbeitsabläufe der Nutzer. Ferner kann der Aufwand für die Durchsetzung und Wartung dieser Maßnahme im Allgemeinen verringert werden, wenn die IT-Sicherheitspolitik in einer Weise aufgebaut ist, dass die für die Nutzer relevanten Teile im Idealfall an separater Stelle auf eine für die Nutzer angebrachte Weise formuliert sind.

Zunächst hat es den Anschein, dass der hohe Aufwand, der insbesondere bei der Durchsetzung anzunehmen ist, in keinem angemessenen Verhältnis zu dem durch die Maßnahme erzielten Nutzen steht. Es muss aber beachtet werden, dass der Aufwand für die Durchsetzung nur einmal entsteht und nur der Aufwand für die Einführung von Änderungen in der IT-Sicherheitspolitik und neuen Nutzern wiederkehrend auftritt. Bei einer Organisation, bei der wenige neue Nutzer und Änderungen in der IT-Sicherheitspolitik zu erwarten sind, wird daher der Nutzen i.d.R. über einen längeren Zeitraum den Aufwand übertreffen.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Es wurde festgestellt, dass mit dieser Maßnahme sowohl bewussten als auch unbewussten Verstößen der Nutzer vorgebeugt werden kann. Ebenso wie bei der vorher betrachteten Bekanntmachung der IT-Sicherheitspolitik entsteht auch bei dieser Maßnahme ein hoher Aufwand durch die Durchsetzung, während sie die normalen Arbeitsabläufe der Nutzer kaum beeinflusst. Um die Wirkung dieser Maßnahme nicht abzuschwächen, ist es bei der Durchsetzung besonders wichtig, die Einführung auf die Bedürfnisse der Nutzer auszurichten. Auch bei dieser Maßnahme kann angenommen werden, dass bei einer Organisation, bei der wenige neue Nutzer zu erwarten sind, der einmalig auftretende hohe Aufwand der Durchsetzung über einen längeren Zeitraum ausgeglichen und daher ein gutes Verhältnis zwischen Aufwand und Nutzen erreicht werden kann.

Vorbeugung von Angriffen durch Nutzer

Bei dieser Maßnahme konnte gezeigt werden, dass sie aufgrund der speziellen Ausrichtung auf Angriffe durch Nutzer nur einen sehr geringen Nutzen aufweist. Dem gegenüber steht

ein hoher Aufwand, der während der Durchsetzung dieser Maßnahme entsteht, und das Risiko, dass sich die Nutzer pauschal als Angreifer verurteilt fühlen. Daher kann grundsätzlich von einem ungünstigen Verhältnis zwischen Aufwand und Nutzen ausgegangen werden.

Nutzer werden verantwortlich gemacht

Bei dieser Maßnahme wurde festgestellt, dass sie gegen unbewusste und bewusste Verstöße Wirkung zeigen kann. Es ist davon auszugehen, dass sie einen hohen Aufwand bei der Durchsetzung und abhängig vom Grad der Verantwortung, den die Nutzer übernehmen sollen, auch beim Betrieb erzeugt. Ferner bestehen die Risiken, dass die Nutzer überfordert werden, ein Konkurrenzdenken zwischen den Nutzern und im schlimmsten Fall ein Konkurrenzverhältnis zwischen erfahrenen Nutzern und den Administratoren entsteht. Aus diesen Gründen ist auch bei dieser Maßnahme im Allgemeinen von einem ungünstigen Verhältnis zwischen Aufwand und Nutzen auszugehen.

Durchsetzung der Pflichtentrennung

Der Nutzen dieser Maßnahme wird vorwiegend durch die bestehenden Möglichkeiten bestimmt, die Pflichtentrennung und das Prinzip der geringsten Privilegien durchzusetzen. Im Allgemeinen wird ein hoher Aufwand bei der Durchsetzung dieser Maßnahme entstehen, wenn organisatorische Umstellungen z.B. der Arbeitsabläufe notwendig sind. Ein großes Risiko bei dieser Maßnahme besteht darin, dass Nutzer diese Maßnahme zu umgehen versuchen, indem sie z.B. ihre Passworte untereinander bekannt machen, wenn dadurch Arbeitsabläufe effizienter gestaltet werden können. Es kann also festgestellt werden, dass das zu erreichende Verhältnis zwischen Aufwand und Nutzen bei dieser Maßnahme insbesondere von der Umgebung abhängt.

Nutzer melden Sicherheitsvorfälle

Bei dieser Maßnahme konnte festgestellt werden, dass sie grundsätzlich eine breite Wirkung hat, diese aber auf Verwundbarkeiten und Vorfälle eingeschränkt ist, die von Nutzern beobachtet werden können. Es entsteht bei dieser Maßnahme neben dem hohen Aufwand bei der Durchsetzung insbesondere beim Betrieb dadurch Aufwand, dass Nutzer Meldungen erstellen. Schließlich besteht das Risiko, dass Nutzer solche Vorfälle nicht melden, bei denen sie sich nicht sicher sind, ob diese von ihnen oder Kollegen verursacht wurden.

Der Aufwand kann bei dieser Maßnahme den Nutzen schnell übertreffen, wenn die Nutzer in der Lage sind, viele Verwundbarkeiten und Vorfälle zu beobachten und dadurch die Produktivität der Nutzer in einem nicht akzeptablen Rahmen eingeschränkt wird. Dies kann z.B. dadurch verursacht werden, dass Dienste häufig für kurze Zeit ausfallen und jedes Mal sehr viele Nutzer dies melden. Ist es dagegen so, dass das IT-System grundsätzlich stabil und sicher läuft, daher von Nutzern nur selten Beobachtungen gemeldet werden und diesen meist relevante sicherheitskritische Vorfälle zugrunde liegen, so kann angenommen werden, dass der Nutzen den Aufwand dieser Maßnahme über einen längeren Zeitraum übertrifft.

6.4.3 Betrachtung von Interdependenzen zwischen Maßnahmen

Bisher erfolgte eine Betrachtung der Maßnahmen ausschließlich unabhängig voneinander. Zum Abschluss dieses Abschnitts sollen mögliche Auswirkungen bei einem kombinierten Einsatz mehrerer Maßnahmen aufgezeigt werden. Gründe, die dafür sprechen Maßnahmen kombiniert einzusetzen, können z.B. eine sich ergänzende Wirkung sein, die den Nutzen erhöht, oder eine bessere Verteilung des Aufwands, wenn z.B. für verschiedene Maßnahmen ähnliche Voraussetzungen geschaffen werden müssen.

Als Beispiel für einen kombinierten Einsatz sollen hier die Maßnahmen „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“ und „Nutzer melden Sicherheitsvorfälle“ betrachtet werden. Auf der einen Seite kann der Nutzen für die Maßnahme „Nutzer melden Sicherheitsvorfälle“ durch den kombinierten Einsatz erhöht werden, da die Nutzer, dadurch dass sie ein besseres Verständnis haben, grundsätzlich in die Lage versetzt werden, bessere und konkretere Meldungen zu erstellen. Auf der anderen Seite kann der Aufwand für die Maßnahme „Entwicklung eines Verständnisses“ teilweise auch dem Aufwand der Maßnahme „Nutzer melden Sicherheitsvorfälle“ angerechnet werden.

Als weiteres Beispiel sollen die Wechselwirkungen der Maßnahme „Bekanntmachung der IT-Sicherheitspolitik“ auf die anderen Maßnahmen betrachtet werden. Dabei kann zunächst festgestellt werden, dass die Bekanntmachung der IT-Sicherheitspolitik bei vielen Maßnahmen als Voraussetzung gesehen werden kann. So ist es z.B. bei den Maßnahmen „Vorbeugung von Angriffen durch Nutzer“ und “Nutzer werden verantwortlich gemacht“ notwendig, dass den Nutzern die IT-Sicherheitspolitik bekannt gemacht wurde, damit sie wissen, welches Verhalten einen Angriff darstellt bzw. welche Regeln sie in ihrem Verantwortungsbereich durchsetzen müssen. Außerdem kann eine kombinierte Durchsetzung mit der Maßnahme „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“ bei den Nutzern zu einem besseren Verständnis für die in der IT-Sicherheitspolitik festgelegten Regelungen führen.

6.5 Zusammenfassung

In diesem Kapitel sollte die Eignung und das Aufwand-Nutzen-Verhältnis der im Kapitel 5 aufgezeigten Schutzmaßnahmen betrachtet werden. Dazu wurde für die einzelnen Maßnahmen zunächst in verschiedenen Abschnitten die Wirkung (vgl. Abschnitt 6.1), die Risiken (vgl. Abschnitt 6.2) und der Aufwand (vgl. Abschnitt 6.3) betrachtet. Die dabei erzielten Ergebnisse wurden im Abschnitt 6.4 verwendet, um für die Maßnahmen Aussagen über das Aufwand-Nutzen-Verhältnis zu treffen. Dabei konnte folgendes festgestellt werden:

- Bei der Maßnahme „Bekanntmachung der IT-Sicherheitspolitik“ wird der Nutzen insbesondere dann den Aufwand übersteigen, wenn nur wenige Änderungen in der IT-Sicherheitspolitik auftreten und nur wenige neue Nutzer einzuweisen sind.

- Bei der „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen

und Erkennungsmerkmale von Angriffen“ kann ein günstiges Verhältnis auftreten, wenn nur wenige neue Nutzer einzuweisen sind.

- Bei der „Vorbeugung von Angriffen durch Nutzer“ ist insbesondere deshalb ein ungünstiges Aufwand-Nutzen-Verhältnis zu erwarten, da die Einstellung der Nutzer zur Organisation durch diese Maßnahme negativ beeinflusst werden kann.
- Bei der Maßnahme „Nutzer werden verantwortlich gemacht“ sollte den Nutzern keine hohe Verantwortung übertragen werden.
- Bei der „Durchsetzung der Pflichtentrennung“ hängt das Aufwand-Nutzen-Verhältnis insbesondere von der Umgebung ab, in der diese Maßnahme eingesetzt werden soll.
- Bei der Maßnahme „Nutzer melden Sicherheitsvorfälle“ kann nur dann von einem angemessenen Aufwand-Nutzen-Verhältnis ausgegangen werden, wenn das IT-System grundsätzlich stabil und sicher läuft.

Schließlich wurde im Unterabschnitt 6.4.3 aufgezeigt, dass ein kombinierter Einsatz der Maßnahmen zu einer Verstärkung der Wirkung bzw. zu einer günstigeren Verteilung des Aufwands führen kann. Dabei wurde insbesondere die „Bekanntmachung der IT-Sicherheitspolitik“ als Voraussetzung für viele Maßnahmen und die Kombination der „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“ mit der Maßnahme „Nutzer melden Sicherheitsvorfälle“ hervorgehoben.

Kapitel 7

Vergleich der Nutzer einbeziehenden Schutzmaßnahmen mit herkömmlichen Schutzmaßnahmen

- Ziel:
  Vergleich des Nutzens und des Aufwands bei den im Kapitel 5 vorgestellten und herkömmlichen Schutzmaßnahmen.
- Vorgehen:
  1. Einführung relevanter herkömmlicher Schutzmaßnahmen.
  2. Vergleich des Nutzens und des zu betreibenden Aufwands.

In diesem Kapitel sollen herkömmliche Schutzmaßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, in Bezug auf Nutzen und Aufwand mit den in Kapitel 5 aufgezeigten Schutzmaßnahmen verglichen werden. Dazu sollen zunächst im Abschnitt 7.1 herkömmliche Schutzmaßnahmen eingeführt und in Bezug auf Nutzen und Aufwand betrachtet werden. Dann soll im Abschnitt 7.2 der Vergleich mit den im Kapitel 5 vorgestellten Schutzmaßnahmen erfolgen.

7.1 Einführung von herkömmlichen Maßnahmen

In diesem Abschnitt sollen herkömmliche Maßnahmen zur Bekämpfung der in den Szenarien aufgezeigten Vorfälle eingeführt werden. Dabei soll zwischen automatischen, halbautomatischen und nicht automatischen Maßnahmen unterschieden werden. Unter automatischen Maßnahmen sollen solche verstanden werden, bei denen ein Mechanismus grundsätzlich nur auf einem IT-System initialisiert werden muss und dieser dann ohne weiteres Eingreifen durch Personen seine Aufgabe erfüllt (vgl. Unterabschnitt 7.1.1). Dementsprechend sollen unter halbautomatischen Maßnahmen solche verstanden werden, bei denen zur Erfüllung der Aufgaben beim Betrieb eine Unterstützung (z.B. Steuerung oder Auswertung) durch Personen (in der Regel Administratoren) notwendig ist (vgl. Unterabschnitt 7.1.2). Unter nicht automatischen Maßnahmen sollen solche verstanden werden, die nicht mit Unterstützung des IT-Systems automatisiert wurden (vgl. Unterabschnitt 7.1.3).

Für jede der hier vorgestellten Maßnahmen soll zunächst die Funktionsweise und dann die Wirkung, der Aufwand und die mit den Maßnahmen verbundenen Risiken diskutiert werden. Da im Rahmen dieser Arbeit ein Vergleich dieser Maßnahmen mit den im Kapitel 5 eingeführten Maßnahmen durchgeführt werden soll, ist es dabei weniger relevant aufzuzeigen, wie diese Maßnahmen im Detail funktionieren, als vielmehr hervorzuheben, gegen welche Arten von Vorfällen sie wirken und welcher Aufwand bzw. welche Risiken mit dem Einsatz verbunden sind.

7.1.1 Betrachtung von automatischen Maßnahmen

„Firewalls“

„Firewalls“ werden eingesetzt, um an Übergängen zwischen Rechnernetzen Zugriffskontrolle zur Vorbeugung gegen Angriffe und „Audit“[1] zur Erkennung von Angriffen durchsetzen zu können (zu „Firewalls“ vgl. z.B. [CZ95] und [Ell99]). Im Allgemeinen werden „Firewalls“ am Übergang zwischen dem internen Rechnernetz einer Organisation und einem externen Rechnernetz (in der Regel das Internet) eingesetzt. Denkbar ist auch, dass eine „Firewall“ zwischen einem besonders zu schützenden Teil des Rechnernetzes einer Organisation (z.B. der Forschungs- und Entwicklungsabteilung) und dem übrigen Rechnernetz der Organisation eingesetzt wird. Dabei ist es notwendig, dafür zu sorgen, dass die zu überwachende Datenkommunikation zwischen den Rechnernetzen ausschließlich über die „Firewall“ erfolgen kann. Eine Kontrolle des Datenflusses innerhalb eines Rechnernetzes durch eine „Firewall“ ist grundsätzlich nicht möglich.

Als Elemente einer „Firewall“ können grundsätzlich „Packet Screens“ und sog. Bastionen bzw. „Application Gateways“ unterschieden werden. **„Packet Screens“** sollen den an einem Übergang zwischen Rechnernetzen auftretenden Datenverkehr nach vorgegebenen Regeln filtern. Sie können z.B. auf Vermittlungsrechnern wie „Router“ oder „Bridges“ installiert sein, die oft die Verbindung zwischen verschiedenen Rechnernetzen darstellen. Die

[1] Beim „Audit“ werden festgelegte Ereignisse aufgezeichnet (Logging) und nach Erkennungsmerkmalen von sicherheitsrelevanten Vorfällen ausgewertet.

Aufstellung von Filterregeln kann entweder durch Erlaubnis- oder durch Verbotsregeln geschehen. Bei Erlaubnisregeln wird eine Datenkommunikation dann erlaubt, wenn sie durch die Regeln ausdrücklich gestattet ist (Alles das, was nicht erlaubt ist, ist verboten). Bei Verbotsregeln wird eine Datenkommunikation dann verhindert, wenn sie durch die Regeln ausdrücklich nicht gestattet ist (Alles das, was nicht verboten ist, ist erlaubt). Dabei können die Filterregeln basieren auf:

- Quell- oder Zieladressen der Datenpakete, z.B. IP-Adressen,
- Typ eines Datenpakets, z.B. TCP (Transmission Control Protocol), UDP (User Datagram Protocol) oder ICMP (Internet Control Message Protocol),
- „Flags“ der Datenpakete, wie z.B. das Syn-Flag von TCP-Paketen,
- Quell- oder Ziel-„Ports“, dies erlaubt grundsätzlich die Einschränkung der Erreichbarkeit bestimmter Dienste.

Die Möglichkeiten für das „Audit“ sind bei „Packet Screens“ oft eingeschränkt. Dies gilt insbesondere dann, wenn der „Packet Screen“ auf einem „Router“ oder einer „Bridge“ eingerichtet wurde, die hierfür oft keine oder nur wenige Möglichkeiten bieten.

Beim Einsatz einer **Bastion** wird das Rechnernetz einer Organisation im Allgemeinen so aufgebaut, dass die Bastion als einziger Rechner des internen Rechnernetzes vom externen Rechnernetz aus erreichbar ist. Eine Datenkommunikation zwischen Rechnern aus dem Rechnernetz der Organisation und dem externen Rechnernetz ist dann nicht mehr direkt, sondern nur noch per Weiterleitung durch die Bastion möglich. Da Angriffe von außen dadurch grundsätzlich auf die Bastion eingeschränkt sind, ist diese besonders zu sichern und zu überwachen. Damit Nutzer in der Lage sind, Dienste nutzen zu können, die von Server im externen Netz erbracht werden, muss eine der beiden folgenden Möglichkeiten bestehen:

- Nutzer haben einen Zugang auf der Bastion und können die Dienste daher direkt von der Bastion aus nutzen. Diese Variante ist grundsätzlich nicht zu empfehlen, da sie wegen der auf der Bastion bereitzustellenden Nutzerzugänge bzgl. der Sicherheit bedenklich ist und sie ferner von den Nutzern eine Anpassung ihrer Arbeitsabläufe erfordert.
- Auf der Bastion sind „Proxy Server“ (Proxy: engl. Stellvertreter) installiert, die die von den Rechnern der Nutzer kommenden Anfragen „stellvertretend“ an die externen Server stellen und die Antworten entsprechend weiterleiten. Hierbei ist es möglich, zusätzlich einen Filter einzurichten, der abhängig vom verwendeten Anwendungsprotokoll (z.B. Hypertext Transfer Protocol, http) vorgegebene Typen von Daten, z.B. ausführbaren Code, nicht weiterleitet (vgl. z.B. [GG00]). Der Einsatz von „Proxy Server“ sollte für die Nutzer transparent (im Sinne von nicht bemerkbar) geschehen.

Grundsätzlich können keine „Router“ oder „Bridges“ als Bastion eingesetzt werden, da diese nicht in der Lage sind, auf der Ebene der Anwendungen (Schicht 7 des OSI-Modells, vgl.

z.B. [Ker95a, Seite 25ff.]) zu arbeiten. Bei Bastionen bestehen im Allgemeinen deutlich bessere Möglichkeiten des „Audit“ als bei „Packet Screens“. Sehr oft können dazu die von den Anwendungen, hier also z.B. von den „Proxy Server“, zur Verfügung gestellten Möglichkeiten des „Logging“ genutzt werden. Oft werden „Packet Screens“ und Bastionen auch kombiniert eingesetzt.

Bezüglich der Wirkung kann festgestellt werden, dass mit einer „Firewall“ grundsätzlich nur solchen Vorfällen entgegengewirkt werden kann, die sich über eine durch eine „Firewall“ geschützte Grenze zwischen zwei Rechnernetzen hinweg auswirken würden. Im Folgenden sollen die im Kapitel 4 in den Szenarien aufgezeigten Vorfälle betrachtet werden, denen durch den Einsatz einer „Firewall“ grundsätzlich entgegengewirkt werden kann:

- **Szenario 6: Dateien im Anhang von Emails werden geöffnet**
  Sind Anhänge von Emails für die Erfüllung der Aufgaben nicht notwendig, so können diese generell beim Passieren der „Firewall“ herausgefiltert werden. Grundsätzlich können dabei auch nur bestimmte Typen von Daten herausgefiltert werden. Es ist allerdings zu beachten, dass der Typ einer Datei nicht immer eindeutig bestimmt werden kann. So kann die Endung einer Datei einfach geändert oder eine Datei in einer Datei anderen Typs z.B. einem Datei-Archiv eingebunden werden.

- **Szenario 8: Teile des IT-Systems können entwendet werden**
  Hier kann der Fall betrachtet werden, in dem Daten über das Rechnernetz nach außen transportiert werden sollen. Ist es für die Erfüllung der Aufgaben nicht oder nur in einem sehr eingeschränkten Rahmen notwendig, Daten in das externe Netz zu transportieren, so können die Möglichkeiten hierfür durch Filterung stark eingeschränkt oder die Nutzung dieser Möglichkeiten durch „Audit“ stark überwacht werden.

- **Szenario 9: Missbrauch des IT-Systems für private Zwecke**
  Sofern der Missbrauch externe Dienste betrifft, die für die Erfüllung der Aufgaben nicht benötigt werden, kann ihre Verfügbarkeit im Rechnernetz der Organisation durch Filterung unterbunden werden.

- **Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus**
  Sofern es sich um einen externen Angreifer handelt, der über das Rechnernetz auf den Zugang eines Nutzers zugreift, können Möglichkeiten des Zugriffs auf die Zugänge des IT-Systems von außen durch eine „Firewall“ eingeschränkt werden.

Aufwand entsteht durch diese Maßnahme oft nur für Administratoren, die für die Einrichtung und Wartung zuständig sind. Für Nutzer ist eine „Firewall“ im Allgemeinen transparent. Alle für die Erfüllung der Aufgaben notwendigen Dienste sollten ohne Änderungen in der Art der Nutzung zur Verfügung stehen (alle nicht notwendigen Dienste im Gegensatz dazu unterbunden werden). Bei einer „Firewall“ können grundsätzlich Möglichkeiten zur Umgehung vorhanden sein, die ihre Ursache z.B. in Fehlern im Aufbau und der Konfiguration der „Firewall“ oder auch in Fehlern in der verwendeten Software haben können. Zum Beispiel kann beim Einsatz von Verbotsregeln eine unangemessene Auswahl von Filterregeln getroffen werden.

Maßnahmen zur Kontrolle der Verwendung von Passworten

Bei der Authentisierung durch Passworte können ergänzend Kontrollsysteme eingesetzt werden, die eine Auswahl schwacher Passworte und eine zyklische Verwendung von Passworten unterbinden bzw. eine regelmäßige Änderung der Passworte überwachen sollen. Um eine Auswahl schwacher Passworte zu unterbinden, werden solche Passworte abgelehnt, die vorgegebenen Regeln entsprechen. Die zyklische Verwendung von Passworten kann durch eine Speicherung bereits verwendeter Passworte realisiert werden. Dabei wird i.A. nur eine bestimmte Anzahl Passworte gespeichert. Bei einer regelmäßigen Änderung kann grundsätzlich nicht nur der Zeitraum, nach dem ein Passwort spätestens geändert werden muss, sondern auch ein Zeitraum, nach dem ein gewähltes Passwort frühestens wieder geändert werden kann, festgelegt werden. Mit einer minimalen Verwendungsdauer für Passworte soll insbesondere verhindert werden, dass Nutzer nach Ablauf der maximalen Verwendungsdauer ihr Passwort innerhalb kurzer Zeit so oft ändern, bis sie ihr vorheriges Passwort wieder verwenden können, da es aus der Liste bereits verwendeter Passworte gelöscht wurde.

Mit derartigen Kontrollsystemen kann der Auswahl schwacher Passworte, wie sie im **Szenario 1: Es werden sehr einfache Passworte benutzt** angedeutet wurde, entgegengewirkt werden. Aufwand entsteht hier im Allgemeinen nur für die Administratoren durch die Einrichtung und Wartung dieser Systeme. Die Nutzer sollten in der Regel keinen Mehraufwand zu dem in der IT-Sicherheitspolitik von ihnen erwarteten Verhalten haben. Durch einen nicht angemessenen Einsatz dieser Systeme kann allerdings das Risiko erhöht werden, dass Nutzer Passworte aufschreiben oder zyklisch wiederverwenden. Dies kann z.B. geschehen, wenn die maximale Verwendungsdauer der Passworte zu kurz angesetzt wird.

„Single Sign On“

Um Situationen zu vermeiden, in denen sich Nutzer gegenüber verschiedenen von ihnen verwendeten Diensten jeweils einzeln authentisieren müssen, können Systeme eingesetzt werden, bei denen ein sog. **„Single Sign On“** möglich ist Dabei müssen sich Nutzer nur einmal gegenüber einem IT-System authentisieren. Die Authentisierung gegenüber anderen Diensten wird dann für die Nutzer transparent durch das IT-System durchgeführt. Eine Möglichkeit, ein „Single Sign On“-Konzept zu realisieren, bietet z.B. Kerberos (vgl. [Eck01, Seite 358ff.]).

Dadurch dass sich Nutzer nicht mehrere Passworte für das IT-System der Organisation merken müssen, können grundsätzlich die im **Szenario 3: Passworte werden mehrfach benutzt** und im **Szenario 4: Passworte werden vergessen** aufgezeigten Vorfälle begrenzt werden. Es muss aber beachtet werden, dass Nutzer oft auch Passworte für andere Zugänge (z.B. privater Email-Zugang) benötigen und es daher immer noch möglich ist, dass Passworte z.B. mehrfach verwendet werden. Außerdem ist es notwendig, hier ein sehr starkes Verfahren zur Authentisierung einzusetzen, da mit der Überwindung dieses Verfahrens alle von einem Nutzer zugreifbaren Dienste und u.U. auch sehr sicherheitskritische Dienste von einem Angreifer missbraucht werden können. In diesem Zusammenhang sei auf die im Folgenden vorgestellten Alternativen zur Authentisierung durch Wissen verwiesen.

Alternativen zur Authentisierung durch Wissen

Bisher wurde ausschließlich die Verifikation der Identität durch Wissen betrachtet. Bereits im Unterabschnitt 4.3.1 wurde darauf hingewiesen, dass eine Verifikation der Identität der Nutzer gegenüber einem IT-System außerdem durch Besitz, Merkmale oder auch durch Ort und Zeit geschehen kann (vgl. hierzu z.B. [Kro02]). Bei der Überprüfung von **Besitz** können z.B. Gegenstände wie Schlüssel, Magnet- bzw. Chipkarten oder auch digitale Signaturen (zu digitalen Signaturen vgl. z.B. [Sta98, Seite 299ff.]) eingesetzt werden. Bei biometrischen Verfahren wird das Vorhandensein bestimmter **Merkmale** überprüft. Dies kann z.B. ein Fingerabdruck, ein Iris-Scan oder auch die Stimme sein. Bei der Überprüfung von **Ort und Zeit** kann eine Einschränkung des Zugriffs über den Ort (z.B. kein Zugriff über ein Rechnernetz) oder der Zeit (z.B. Zugriff nur Montags bis Freitags von acht bis achtzehn Uhr) erfolgen. Diese Verfahren können auch kombiniert eingesetzt werden. So ist es häufig üblich, Besitz und Wissen zu überprüfen. Als Beispiel seien Chipkarten mit einer PIN (Persönliche Identifikationsnummer) genannt. Ferner ist es denkbar, Besitz und Eigenschaft zu überprüfen. Dies kann z.B. in Form von Chipkarte und Iriserkennung durchgeführt werden. Grundsätzlich ist hierbei möglich, für verschiedene Teile eines IT-Systems mit verschieden hohen Schutzbedarf unterschiedliche Verfahren oder Kombinationen von Verfahren einzusetzen, die dem jeweils notwendigen Schutzbedarf gerecht werden.

Erfolgt der Einsatz der hier vorgestellten Verfahren als Alternative zu oder in Kombination mit Passwort-Abfragen, kann den in den Szenarien aus dem Bereich der unangemessenen Verwendung von Passworten aufgezeigten Vorfällen entgegengewirkt werden:

- **Szenario 1: Es werden sehr einfache Passworte benutzt**
  Wird bei einem kombinierten Einsatz mehrerer Verfahren ein schwaches Passwort benutzt und dieses von einem Angreifer ermittelt, so muss dieser immer noch die verbleibenden Verfahren überwinden. Bei einem kombinierten Einsatz mit einer Chipkarte würde dies also bedeuten, dass der Angreifer die Chipkarte z.B. entwenden oder nachbilden müsste. Dieses Vorgehen bietet also grundsätzlich einen höheren Grad von Sicherheit. Es besteht aber das Risiko, dass Nutzer im Bewusstsein, dass diese nicht die einzige von einem Angreifer zu überwindende Hürde darstellen, schwache Passworte wählen, was zu einem insgesamt schlechteren Sicherheitsniveau führen kann.

- **Szenario 2: Passworte werden aufgeschrieben**,
  Szenario 3: Passworte werden mehrfach benutzt
  und **Szenario 4: Passworte werden vergessen**
  Werden die hier vorgestellten Verfahren in Kombination mit Passworten benutzt, so wird grundsätzlich ein höherer Grad von Sicherheit erreicht. Die im Kapitel 4 aufgezeigten Probleme können aber weiterhin bestehen bleiben. So ist es bei einem kombinierten Einsatz mit einer Chipkarte z.B. denkbar, dass das Passwort oder die PIN auf der Chipkarte vermerkt wird. Werden mehrere Passworte benötigt, ist es auch weiterhin möglich, dass ein Passwort mehrfach verwendet wird. Schließlich ist es auch bei einem kombinierten Einsatz möglich, dass Passworte vergessen werden. Werden die hier vorgestellten Mechanismen als Alternative verwendet, so sind Passworte

nicht mehr notwendig und die hiermit verbundenen Probleme entfallen. Stattdessen müssen die Risiken betrachtet werden, die mit dem Einsatz der hier vorgestellten Mechanismen verbunden sind. Diese sind im Folgenden noch zu behandeln.

Beim Einsatz dieser Verfahren entsteht zunächst Aufwand durch die Einrichtung und Wartung. Insbesondere sind dabei auch die Kosten für die Anschaffung spezieller Hardware wie Chipkartenleser oder Fingerabdruckscanner zu berücksichtigen. Die Verfahren sollten so implementiert werden, dass für die Nutzer kein deutlich höherer Aufwand bei der Authentisierung entsteht. Bei den hier betrachteten Mechanismen können Risiken dadurch entstehen, dass Gegenstände gestohlen bzw. dupliziert und Merkmale nachgebildet werden können. Bei der Biometrie besteht hierbei insbesondere das Problem, dass das zu überprüfende Merkmal wie z.B. ein Fingerabdruck im Gegensatz zu Passworten oder Gegenständen nicht beliebig oft ausgetauscht werden kann. Ferner sind die in diesem Bereich zur Verfügung stehenden Techniken bisher noch nicht ausgereift.

7.1.2 Betrachtung von halbautomatischen Maßnahmen

„Intrusion Detection Systems“ (IDS) und „Intrusion Response Systems“ (IRS)

Mit dem Einsatz von „Intrusion Detection Systems“ wird als Ziel die Erkennung von Angriffen verfolgt (zu IDS vgl. z.B. [Irr01, Seite 47ff.]). Dabei werden verschiedene Größen des zu sichernden Zielsystems laufend überwacht und ausgewertet. Grundsätzlich können zwei Varianten der Auswertung unterschieden werden:

- Bei der Signaturanalyse werden dem IDS Charakteristika für Angriffe vorgegeben und diese mit den aktuellen Zuständen des IT-Systems verglichen.
- Bei der Anomalieerkennung lernt das IDS zunächst das normale Verhalten kennen und versucht dann Abweichungen von dem normalen Verhalten eines Nutzers oder des IT-Systems zu entdecken.

Beim Einsatz von IDS wird insbesondere versucht einen Angriff sehr schnell zu erkennen, so dass nicht nur eine Rekonstruktion des Hergangs nach erfolgtem Angriff (post mortem), sondern die Einleitung von Gegenmaßnahmen während des Angriffs möglich ist. In diesem Zusammenhang können IDS unterschieden werden in passive und aktive Systeme. Bei passiven Systemen werden keine eigenständigen Gegenmaßnahmen ergriffen, es erfolgt lediglich eine Alarmierung. Aktive Systeme werden auch als „Intrusion Response Systems“ bezeichnet. Bei IRS können zusätzlich eigenständige Gegenmaßnahmen ausgelöst werden, wie z.B. das Schließen von Netzwerkverbindungen und die Sperrung von Nutzerzugängen.

Mit dem Einsatz von IDS und IRS kann den folgenden im Kapitel 4 in den Szenarien aufgezeigten Vorfällen entgegengewirkt werden:

- **Szenario 9: Missbrauch des IT-Systems für private Zwecke**
  Der Missbrauch eines IT-Systems kann dann erkannt werden, wenn bei einem auf Signaturanalyse basierenden System die konkrete Art des Missbrauchs vorgegeben

wurde oder dieser bei Anomalie erkennenden Systemen von dem normalen Verhalten abweicht. Es ist bei Anomalie erkennenden Systemen hierbei zu beachten, dass der Missbrauch nicht erkannt werden kann, wenn er in der Phase des Einlernens bereits durchgeführt wurde und daher als normales Verhalten angesehen wird.

- **Szenario 10: „Salamiangriff“**
  Die zugrunde liegende Idee bei einem „Salamiangriff“ ist es, die einzelnen Schritte gerade so klein zu halten, dass sie nicht entdeckt werden. Obwohl derartige Angriffe von IDS grundsätzlich entdeckt werden können, besteht die Möglichkeit, dass die einzelnen Schritte von einem Angreifer so klein gewählt werden, dass sie die vorgegebene Toleranzgrenze nicht überschreiten.

- **Szenario 11: Dienste stehen nicht mehr zur Verfügung**
  Durch IDS kann z.B. plötzlich steigender Datenverkehr im Rechnernetz oder steigende Nachfrage nach einem Dienst registriert und als potentieller „Denial of Service“-Angriff (DoS-Angriff) gewertet werden.

- **Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus**
  In diesem Fall kann von einem IDS z.B. eine plötzliche Änderung des Verhaltens eines Nutzers registriert und als Angriff gewertet werden.

Aufwand entsteht für Nutzer beim Einsatz eines solchen Systems im Allgemeinen nicht. Im schlimmsten Fall können so genannte „False Positive“-Fehler, also Fälle, in denen vom IDS ein vermeintlicher Angriff erkannt wird, obwohl keiner stattfindet, dazu führen, dass die Arbeit von Nutzern z.B. durch Gegenmaßnahmen beeinträchtigt oder unterbrochen wird. Grundsätzlich stellen derartige „False Positive“-Fehler ein Risiko dar. Dies gilt insbesondere bei IRS, bei denen automatisch Gegenmaßnahmen ausgelöst werden können. Weitere Risiken sind so genannte „False Negative“-Fehler, bei denen ein durchgeführter Angriff nicht erkannt wird, da er z.B. bei der Signaturanalyse nicht vorgegeben wurde oder bei der Anomalieerkennung nicht als nicht normal erkannt wurde. Ferner besteht beim Einsatz von IDS das Problem, dass bei der Auswertung der Daten zur Erkennung von Angriffen die Vertraulichkeit personenbezogener Daten nicht verletzt werden darf.

„Antimalware“-Software

Unter „Malware“ wird im Allgemeinen Software verstanden, die intendierte Funktionen besitzt, die aus Sicht der Nutzer oder des Betreibers eines IT-Systems unerwartet oder unerwünscht sind (vgl. [Pfl96, Seite 179]). „Malware“ kann unterschieden werden in:

- Viren:
  Viren zeichnen sich dadurch aus, dass sie in der Lage sind, sich auf nicht mit dem Viren-Code „infizierte“ Daten zu übertragen, indem sie diese modifizieren. Viren können eine Schadfunktion haben, die oft als „Payload“ bezeichnet wird. Diese Schadfunktion kann durch verschiedene Bedingungen zur Ausführung gebracht (getriggert)

werden. Unter „Logischen Bomben“ werden Schadfunktionen verstanden, die ausgeführt werden, wenn ein bestimmter Zustand auftritt. Dies kann z.B. das Starten eines bestimmten Prozesses sein. Unter „Zeitbomben“ werden Schadfunktionen verstanden, die zu einem vorgegebenen Zeitpunkt ausgeführt werden.

- Trojanische Pferde:
  Unter Trojanischen Pferden werden Programme verstanden, die neben von einem Nutzer erwarteten und erwünschten Funktionen auch weitere von einem Nutzer nicht erwartete und nicht erwünschte Funktionen haben.

- Würmer:
  Würmer sind Programme, die sich in einem Rechnernetz ausbreiten, indem sie Kopien auf anderen Rechnern zur Ausführung bringen. Ebenso wie Viren können sie eine Schadfunktion mit sich führen.

Mit „Antimalware“-Software soll das Auftreten von „Malware“ in einem IT-System erkannt oder diesem vorgebeugt werden. Grundsätzlich kann dabei zwischen „On Access Scanner“ und „On Demand Scanner“ unterschieden werden. Bei „On Access Scanner“ wird vor dem Ausführen eines Programms oder dem Verarbeiten von Daten ein „Scanner“ aufgerufen, der nach „Malware“ sucht und gegebenenfalls die Ausführung bzw. die Verarbeitung abbricht. Bei „On Demand Scanner“ erfolgt ein expliziter Aufruf eines „Scanner“, um das ganze oder Teile des IT-Systems nach dem Vorhandensein von Malware zu durchsuchen.

Durch „Antimalware“-Software kann den folgenden im Kapitel 4 aufgezeigten Vorfällen entgegengewirkt werden:

- **Szenario 6: Dateien im Anhang von Emails werden geöffnet**
  Emails können durch „On Access Scanner“ auf das Vorhandensein von „Malware“ überprüft und gegebenenfalls verworfen werden.

- **Szenario 8: Teile des IT-Systems können entwendet werden**
  Grundsätzlich ist es möglich, durch „Malware“ Passworte oder andere Daten auszuspionieren. Dies kann z.B. durch ein „Trojanisches Pferd“ geschehen oder Teil der Schadfunktion eines Virus oder Wurms sein. Der Einsatz von „Antimalware“-Software kann derartigen Angriffen entgegenwirken.

Für Administratoren entsteht Aufwand durch die Einrichtung, Wartung (z.B. Aktualisierung der zur Erkennung verwendeten Signaturen) und dem Betrieb der „Antimalware“-Software. Für die Nutzer sollte kein zusätzlicher Aufwand entstehen, da „On Access Scanner“ automatisch ohne weitere Aktionen der Nutzer aufgerufen werden (hierdurch kann es allerdings zu Verzögerungen kommen) und eine regelmäßige Überprüfung des IT-Systems auf „Malware“ durch „On Demand Scanner“ die Aufgabe von Administratoren sein sollte. Durch den Einsatz von „Antimalware“-Software kann das Gefühl einer „falschen Sicherheit“ entstehen, das z.B. dazu führen kann, dass auch nicht vertrauenswürdige Programme ausgeführt bzw. Dateien geöffnet werden, da man sich darauf verlässt, dass die „Antimalware“-Software jegliche „Malware“ erkennen wird.

Redundante Auslegung von Diensten und Server

Mit einer redundanten Auslegung von Server soll grundsätzlich die Verfügbarkeit der von ihnen erbrachten Dienste erhöht werden. Eine redundante Auslegung bedeutet hierbei, dass mehrere Komponenten mit derselben Funktionalität bereitgestellt werden, so dass beim Ausfall einer Komponente andere ihre Aufgaben übernehmen können. Grundsätzlich kann bei der redundanten Auslegung zwischen den sog. „heißen“ und „kalten Reserven“ unterschieden werden (vgl. [Lal01, Seite 171]). Bei „heißen Reserven“ sind alle verfügbaren Komponenten im Betrieb, so dass bei Ausfall einer Komponente eine sehr schnelle Übernahme der Aufgaben möglich ist. Bei „kalten Reserven“ werden redundante Komponenten erst bei einen konkreten Ausfall in Betrieb genommen. Das kann bedeuten, dass sie vorgehalten werden und bei einem Ausfall nur gestartet werden müssen, es ist aber auch denkbar, dass Komponenten erst noch eingerichtet oder sogar beschafft werden müssen. Grundsätzlich ist festzuhalten, dass die Vorhaltung einer „heißen Reserve“ im Allgemeinen höhere Kosten verursacht als eine „kalte Reserve“. Hier muss für den Einzelfall in Abhängigkeit von der Ausfallwahrscheinlichkeit, der erwarteten Ausfalldauer und der bei einem Ausfall entstehenden Kosten entschieden werden, welche der Varianten zu wählen ist.

Wichtig sind im Zusammenhang mit einer redundanten Auslegung auch Maßnahmen zur Wiederherstellung der Verfügbarkeit. Wird die Verfügbarkeit ausgefallener Komponenten nicht in angemessener Zeit wiederhergestellt, kann der Fall eintreten, dass alle Komponenten ausgefallen sind, bevor die Verfügbarkeit einer ausgefallenen Komponente wiederhergestellt werden konnte.

Eine redundante Auslegung von Server soll die Verfügbarkeit der von diesen erbrachten Dienste erhöhen. Sie kann damit dem in **Szenario 11: Dienste stehen nicht mehr zur Verfügung** aufgezeigten Vorfall entgegenwirken. Dabei kann die redundante Auslegung von Diensten oft in einer Weise geschehen, dass sie für die Nutzer transparent ist und für sie daher keinen zusätzlichen Aufwand nach sich zieht. Allerdings zieht eine redundante Auslegung einen höheren Aufwand bei der Administration der Server nach sich.

Kryptographische Verfahren

Traditionell soll mit kryptographischen Verfahren dem Abhören von Kommunikationsbeziehungen entgegengewirkt werden (zu kryptographischen Verfahren vgl. z.B. [Pfl96, Seite 21ff.]). Grundsätzlich kann durch kryptographische Verfahren aber auch die Integrität von Daten und die Authentizität von Sendern gesichert werden. Im Zusammenhang mit den im Kapitel 4 aufgestellten Szenarien soll im Folgenden allerdings nur der Aspekt des Schutzes vor dem Abhören von Kommunikationsbeziehungen betrachtet werden. Dabei soll einem Sender ermöglicht werden, eine Nachricht über ein nicht geschütztes Übertragungsmedium zu einem Empfänger zu übertragen, ohne dass ein Angreifer die Möglichkeit hat, Kenntnis vom Inhalt der Nachricht zu erlangen. Dazu wird der Klartext der Nachricht mit einem kryptographischen Verfahren in einen Kryptotext überführt. Da dies im Allgemeinen in Abhängigkeit von einem Schlüssel geschieht, spricht man hier auch von Verschlüsselung. Der Kryptotext kann dann vom Sender über das nicht geschützte Übertragungsmedium

zum Empfänger übertragen werden. Fängt ein Angreifer die Übertragung ab, kann dieser den Klartext nicht ohne Weiteres daraus ableiten. Grundsätzlich wird davon ausgegangen, dass dem Empfänger sowohl das kryptographische Verfahren als auch der zur Wiederherstellung des Klartextes notwendige Schlüssel bekannt ist. Damit ist dieser in der Lage, den Klartext aus dem Kryptotext wiederherzustellen, man spricht auch von Entschlüsselung.

Grundsätzlich werden symmetrische und asymmetrische Verfahren unterschieden. Werden zur Ver- und Entschlüsselung die gleichen Schlüssel verwendet, so spricht man von **symmetrischen Verfahren**. Werden verschiedene Schlüssel verwendet, so spricht man von **asymmetrischen Verfahren**. Dabei sind asymmetrische Verfahren so aufgebaut, dass es zusammen gehörende Schlüsselpaare bestehend aus einem öffentlichen und einem privaten Schlüssel gibt. Der Sender benutzt den öffentlichen Schlüssel des Empfängers, um die Nachricht zu verschlüsseln, und nur dieser kann diese mit seinem geheim gehaltenen privaten Schlüssel wieder entschlüsseln.

Im Zusammenhang mit der Übertragung von Daten in Rechnernetzen kann grundsätzlich zwischen Punkt-zu-Punkt- und Ende-zu-Ende-Verschlüsselung unterschieden werden (vgl. [Pfl96, Seite 406ff.]). Bei einer **Ende-zu-Ende-Verschlüsselung** werden die zu übertragenden Daten beim Sender verschlüsselt und beim Empfänger wieder entschlüsselt (vgl. Abbildung 7.1). Dies kann manuell durch die Nutzer oder (halb-)automatisch durch das IT-System geschehen. Ein großer Nachteil dieser Vorgehensweise ist, dass die zur Übermitt-

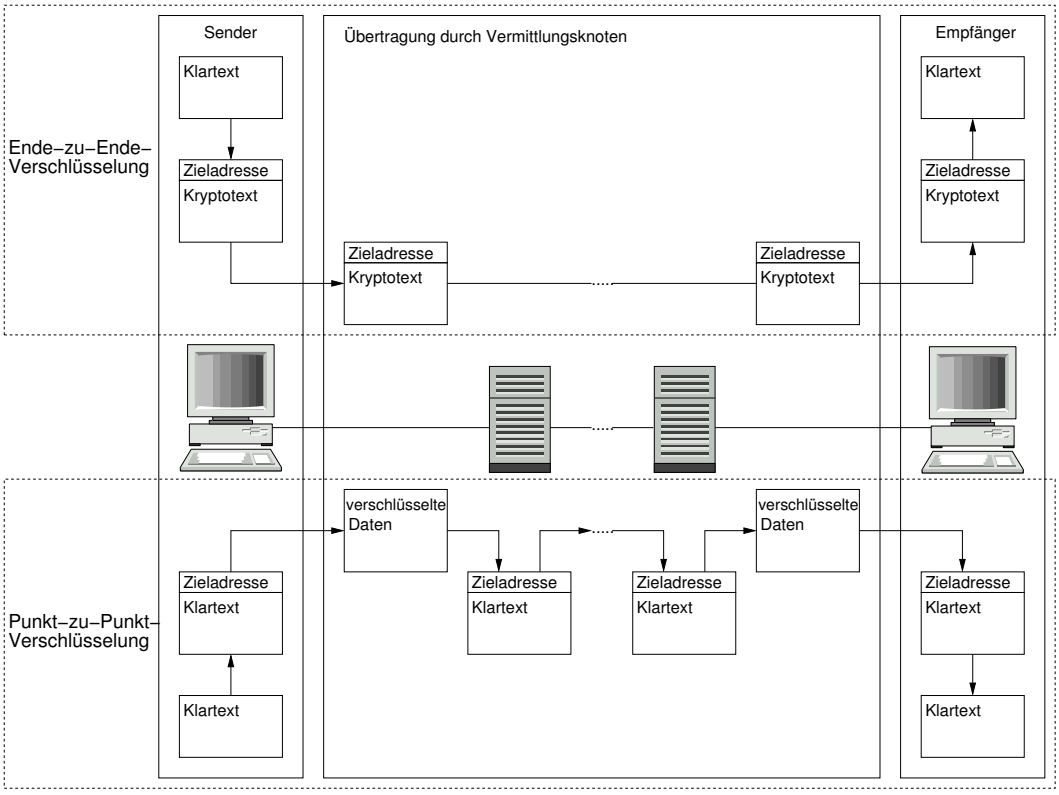


Abbildung 7.1: Ende-zu-Ende- und Punkt-zu-Punkt-Verschlüsselung

lung notwendigen Informationen wie z.B. die Adresse des Empfängers nicht verschlüsselt werden können. Als ein Spezialfall von Ende-zu-Ende-Verschlüsselung können „Virtual Private Networks“ (VPNs) angesehen werden. Eine typische Einsatzmöglichkeit für VPNs ist die Verbindung von örtlich getrennten Teilen des Rechnernetzes einer Organisation über unsichere Kommunikationsmedien wie z.B. das Internet. Dabei wird der gesamte zwischen den beiden Teilnetzen ausgetauschte Datenverkehr am Übergang zum unsicheren Kommunikationsmedium ver- bzw. entschlüsselt. Bei einer **Punkt-zu-Punkt-Verschlüsselung** findet eine Verschlüsselung der Daten nicht vom Sender zum Empfänger, sondern zwischen im Netzwerk direkt kommunizierenden Rechnern statt. Auf diese Weise ist es möglich, auch die Zielinformationen zu verschlüsseln. Der Nachteil bei diesem Verfahren ist allerdings, dass in den Vermittlungsrechnern, die sich auf dem Übertragungsweg befinden, die unverschlüsselten Daten abgehört werden können.

In dem hier betrachteten Zusammenhang sollen kryptographische Verfahren als Möglichkeit des Schutzes vor dem Abhören der Inhalte von Kommunikationsbeziehungen, wie es im **Szenario 13: Kommunikationsbeziehungen werden belauscht** aufgezeigt wurde, gesehen werden. Dabei muss beachtet werden, dass durch den Einsatz von kryptographischen Verfahren im Allgemeinen nicht das Vorhandensein von Kommunikationsbeziehungen verborgen wird. Für die Nutzer kann durch den Einsatz von kryptographischen Verfahren Aufwand entstehen, z.B. wenn eine Ende-zu-Ende-Verschlüsselung zwischen Nutzern stattfindet, bei der ein explizites Ver- und Entschlüsseln notwendig ist (z.B. Ver- und Entschlüsseln von Emails). Generell erzeugen kryptographische Verfahren Aufwand bei der Ver- und Entschlüsselung. Dadurch können Verzögerungen bei der Übermittlung von Daten entstehen. Dies kann insbesondere bei interaktiven Anwendungen zu von den Nutzern nicht tolerierten Verzögerungen führen, die Versuche zur Umgehung der kryptographischen Verfahren nach sich ziehen können. Dieses Risiko besteht vor allem bei manuellen oder halbautomatischen Maßnahmen, bei denen die Anwendung von kryptographischen Verfahren zusätzliche Aktionen der Nutzer voraussetzt.

7.1.3 Betrachtung von nicht automatischen Maßnahmen

Physikalische Maßnahmen

Der Einsatz von physikalischen Maßnahmen hat im Allgemeinen das Ziel, das IT-System vor Umgebungseinflüssen zu schützen und einen physischen Zugangsschutz zum IT-System zu gewährleisten. In der Tabelle 7.1 sind einige Bedrohungen aufgelistet, denen mit physikalischen Maßnahmen entgegengewirkt werden soll. Im Folgenden sollen einige Beispiele für physikalische Maßnahmen gegeben werden. Dabei wird eine Unterscheidung in vorbeugende, erkennende und korrigierende Maßnahmen durchgeführt.

Beispiele für vorbeugende Schutzmaßnahmen:

- Auswahl eines geeigneten Grundstücks
  Dabei sollte die Wahrscheinlichkeit für Katastrophen wie Überschwemmungen oder Erdbeben und Besonderheiten der Umgebung wie Entfernung zu Chemie- oder Atomkraftwerken, aber auch zu Polizei- und Feuerwehrstationen berücksichtigt werden.

Umgebungseinflüsse		Zugang
Feuer	Erschütterungen	Diebstahl
Rauch	Wasser	Vandalismus
Feuchtigkeit	Erdbeben	Sabotage
Temperatur	Sturm	Spionage
Staub	Stromausfälle	

Tabelle 7.1: Bedrohungen gegen die physikalische Maßnahmen wirken

- Angemessene Gestaltung der Gebäude und Räume
  Hierbei sind z.B. die Zugänge zu Gebäuden und Räumen (welche Zugänge gibt es, wie werden sie geschützt), die Lage von Fenstern, Brandschutzmauern oder Wasserleitungen und eine zweckmäßige Nutzung der Räume (z.B. sollten Server-Räume besonders gut gesichert sein, sie sollten nicht zur Aufbewahrung großer Mengen leicht entflammbarer Materialien wie Papier dienen) zu betrachten.

- Sicherung der Hardware vor Diebstahl
  Teile der Hardware können an nicht oder nur schwer beweglichen Gegenständen angeschlossen werden, Rechnergehäuse können vor einer nicht autorisierten Öffnung geschützt werden, Möglichkeiten zur Nutzung von Wechselmedien, wie z.B. Diskettenlaufwerke, können entfernt werden und verwendete Wechselmedien, wie Disketten, aber insbesondere auch Backup-Medien, können in verschlossenen Schränken o.ä. aufbewahrt werden.

Beispiele für erkennende Schutzmaßnahmen:

- Installation von Feuer- bzw. Rauchmeldern
  Dabei sollten Feuer- und Rauchmelder nicht nur in Räumen, sondern auch in Kabelschächten u.Ä. installiert werden, um hier eine unbemerkte Ausbreitung von Feuer oder Rauch zu verhindern. Diese Systeme müssen regelmäßig auf ihre Funktionsfähigkeit überprüft werden.

- Überwachung der Luftfeuchtigkeit und Temperatur
  Dabei sollte bei einer Überschreitung vorgegebener Toleranzgrenzen eine Alarmierung erfolgen.

Beispiele für korrigierende Schutzmaßnahmen:

- Installation von Feuerlöschanlagen
  Hierbei können grundsätzlich Sprinkleranlagen oder Gase wie Kohlendioxid eingesetzt werden. Beim Einsatz von Sprinkleranlagen sollte dafür gesorgt werden, dass vor der Auslösung automatisch der Strom abgeschaltet wird, um Kurzschlüsse zu verhindern. Beim Einsatz von Gasen wie Kohlendioxid besteht oft das Problem, dass sie gesundheitsschädlich oder im schlimmsten Fall sogar tödlich für den Menschen sind. Aus diesem Grund sollte vor dem Ausströmen des Gases eine Alarmgebung erfolgen. Ferner sind derartige Gase oft schädlich für die Umwelt.

Bei physikalischen Maßnahmen kann eine Unterscheidung in drei Sicherungsringe (rings of protection, vgl. [FKB89, Seite117])) erfolgen. Dabei kann Umgebungssicherheit (Perimeter Security), Bereichssicherheit (Area Security) und Punktsicherheit (Point Security) unterschieden werden. Bei der Umgebungssicherheit ist das Ziel, eine Bedrohung außerhalb eines definierten Bereichs zu halten. Dies trifft z.B. bei einem Zutrittsschutz zu Gebäuden zu. Bei der Bereichssicherheit wird der zu schützende Bereich flächendeckend gesichert. Dies geschieht z.B. beim Einsatz von Rauchmeldern. Die Punktsicherheit ist ein Spezialfall der Umgebungssicherheit. Dabei wird innerhalb eines durch Umgebungssicherheit geschützten Bereiches ein besonderer Schutz für Bereiche mit besonders hohem Schutzbedarf durchgeführt. Dies kann z.B. für die Räume gelten, in dem zentrale Server eines IT-Systems untergebracht sind. In der Tabelle 7.2 wird eine mögliche Einteilung der hier aufgezeigten physikalischen Schutzmaßnahmen in diese drei Sicherungsringe aufgezeigt.

	Umgebungs-sicherheit	Bereichs-sicherheit	Punkt-sicherheit
Auswahl eines geeigneten Grundstücks		x	
Angemessene Gestaltung der Gebäude und Räume	x	x	
Sicherung der Hardware vor Diebstahl			x
Installation von Feuer- bzw. Rauchmeldern		x	
Überwachung der Luftfeuchtigkeit und Temperatur		x	
Installation von Feuerlöschanlagen		x	

Tabelle 7.2: Einordnung der physikalischen Maßnahmen in die drei Sicherungsringe

Im Zusammenhang mit den im Kapitel 4 betrachteten Szenarien kann festgestellt werden, dass mit physikalischen Maßnahmen insbesondere den im **Szenario 8: Teile des IT-Systems können entwendet werden** aufgezeigten Vorfällen entgegengewirkt werden kann. Grundsätzlich können physikalische Maßnahmen hohe Kosten bei der Installation nach sich ziehen. Dies gilt insbesondere, wenn sie nachträglich installiert werden. Physikalische Maßnahmen sollten im Allgemeinen keine Auswirkungen auf die Arbeitsabläufe der Nutzer haben. Es ist aber denkbar, dass einige damit verbundene organisatorische Regelungen, wie z.B. schwere Brandschutztüren geschlossen zu halten, die Arbeitsabläufe beeinträchtigen. Es ist ferner denkbar, dass versucht wird diese Regelungen zu umgehen, indem z.B. Brandschutztüren permanent offen gehalten werden.

7.1.4 Fazit

In diesem Unterabschnitt sollen für die in diesem Abschnitt vorgestellten Schutzmaßnahmen die Wirkungen, Risiken und der durch ihren Einsatz entstehende Aufwand noch einmal in einem Überblick aufgezeigt werden. Um die Wirkungen aufzuzeigen, wurden die Schutzmaßnahmen in der Tabelle 7.3 den im Kapitel 4 aufgestellten Szenarien gegenüber gestellt. Die folgenden in der Tabelle zu erkennenden Besonderheiten sollen besonders hervorgehoben werden:

	1	2	3	4	5	6	7	8	9	10	11	12	13
	Automatische Maßnahmen												
„Firewalls“						x		x	x			x	
Passwort-Kontrollsysteme	x												
„Single Sign On“		x		x									
Alternativen zu Passworte	x	x	x	x									
	Halbautomatische Maßnahmen												
IDS / IRS									x	x	x	x	
„Antimalware“-Software						x		x					
Redundante Dienste und Server											x		
kryptographische Verfahren													x
	Nicht automatische Maßnahmen												
Physikalische Maßnahmen								x					

Szenario 1: Es werden sehr einfache Passworte benutzt
Szenario 2: Passworte werden aufgeschrieben
Szenario 3: Passworte werden mehrfach benutzt
Szenario 4: Passworte werden vergessen
Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet
Szenario 6: Dateien im Anhang von Emails werden geöffnet
Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet
Szenario 8: Teile des IT-Systems können entwendet werden
Szenario 9: Missbrauch des IT-Systems für private Zwecke
Szenario 10: „Salamiangriff“
Szenario 11: Dienste stehen nicht mehr zur Verfügung
Szenario 12: Angreifer führt Angriffe vom Zugang eines Nutzers aus
Szenario 13: Kommunikationsbeziehungen werden belauscht

Tabelle 7.3: Gegenüberstellung der Szenarien und Schutzmaßnahmen

- Bei **Szenario 5: Telefonische Anfragen nach Passworten werden beantwortet** und **Szenario 7: Emails mit gefälschten Virus-Warnungen werden weitergeleitet** wirkt keine der hier aufgezeigten Schutzmaßnahmen den dort betrachteten Vorfällen entgegen. Es handelt sich hierbei um Szenarien aus dem Themenbereich der „Social Engineering“-Techniken. In beiden Fällen kann angenommen werden, dass es grundsätzlich nicht möglich ist, herkömmliche Maßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, zu finden, die den Ursachen dieser Vorfälle entgegenwirken, da diesen keine technischen Probleme, sondern psycho-soziologische Aspekte zugrunde liegen. Unter geeigneten Umständen kann es allerdings möglich sein, deren Auftreten in einem eingeschränkten Maße zu erkennen. So können z.B. Rufnummernanzeigen bei Telefonen bedingt helfen, die Herkunft eines Anrufs zu überprüfen.

- Die folgenden der hier aufgezeigten Maßnahmen zeigen nur gegen Vorfälle aus jeweils einem Themenbereich Wirkung: „Maßnahmen zur Kontrolle der Verwendung von Passworten“, „Single Sign On“, „Alternativen zur Authentisierung durch Wissen“, „redundante Auslegung von Diensten und Server“, „Kryptographische Verfahren“ und „physikalische Maßnahmen“.

- Die Maßnahmen „IDS und IRS“ und „Antimalware-Software“ zeigen Wirkung gegen

Vorfälle aus jeweils zwei Themenbereichen.

- „Firewalls“ zeigen Wirkung gegen Vorfälle aus drei Themenbereichen.

Bei dieser Aufstellung der Wirkungen muss aber beachtet werden, dass einige der hier vorgestellten Maßnahmen weitere Wirkungen haben, denen kein entsprechendes Szenario gegenüber gestellt werden kann. Ein Beispiel hierfür ist bei den physikalischen Maßnahmen die Installation von Feuer- und Rauchmeldern. Dies kann u.a. damit begründet werden, dass derartige Szenarien nicht den im Abschnitt 4.2 aufgestellten Anforderungen an die im Rahmen der Arbeit betrachteten Szenarien entsprechen würden.

Im Folgenden sollen die Risiken betrachtet werden, die der Einsatz der in diesem Abschnitt eingeführten Schutzmaßnahmen nach sich ziehen kann. Bei vielen Maßnahmen ist es möglich, dass eine nicht angemessene Implementierung oder Konfiguration der Schutzmaßnahmen zu einer eingeschränkten Wirksamkeit führen kann. Bezüglich der Nutzer sind insbesondere Möglichkeiten und Ursachen zur Umgehung der Maßnahmen zu betrachten. So ist auch bei den hier betrachteten Schutzmaßnahmen zu erwarten, dass Nutzer versuchen werden, diese zu umgehen, wenn sie ihre Arbeitsabläufe behindern oder verzögern. Als Seiteneffekte beim Einsatz dieser Schutzmaßnahmen können z.B. Situationen betrachtet werden, bei denen aus Vertrauen auf die technischen Schutzmaßnahmen andere Vorsichtsmaßnahmen vernachlässigt werden. Ein derartiger Fall wurde z.B. bei der Betrachtung der „Antimalware“-Software angedeutet: Im Vertrauen auf die Wirkung der „Antimalware“-Software werden auch Dokumente unbekannter Herkunft geöffnet.

Bezüglich des durch den Einsatz der Schutzmaßnahmen entstehenden Aufwands kann festgestellt werden, dass durch die Einrichtung und die Wartung dieser zwar Aufwand für die Administratoren entsteht, sie im Allgemeinen aber so eingerichtet werden können, dass für die Nutzer kein oder nur ein geringer Mehraufwand entsteht. Es ist allerdings zu beachten, dass durch die Schutzmaßnahmen unter Umständen Möglichkeiten eingeschränkt werden, die die Arbeitsabläufe der Nutzer vereinfachen und damit ihre Produktivität erhöhen könnten, weil die Risiken der Bereitstellung als zu hoch angesehen werden.

7.2 Vergleich der Schutzmaßnahmen

In diesem Abschnitt soll ein Vergleich zwischen den im Kapitel 5 aufgezeigten und den im vorhergehenden Abschnitt vorgestellten Schutzmaßnahmen durchgeführt werden. Dabei sollen Aspekte aufgezeigt werden, die bei der Auswahl eines umfassenden, aus verschiedenen Arten von Schutzmaßnahmen bestehenden Sicherheitskonzeptes berücksichtigt werden müssen. Dazu soll eine Aufteilung der zu betrachtenden Aspekte in die folgenden Bereiche vorgenommen werden (vgl. Abschnitt 3.2):

- Erstellung einer IT-Sicherheitspolitik:
  Bewertung und Auswahl der einzusetzenden Schutzmaßnahmen

- Durchsetzung einer IT-Sicherheitspolitik:
  Implementierung, Bekanntmachung und Akzeptanz der gewählten Schutzmaßnahmen

- Betrieb und Wartung der Schutzmaßnahmen:
  Angemessenheit der Schutzmaßnahmen, durch sie entstehender Aufwand

7.2.1 Bewertung und Auswahl der einzusetzenden Schutzmaßnahmen

In diesem Unterabschnitt sollen Aspekte betrachtet werden, die bei der Bewertung und Auswahl der einzusetzenden Schutzmaßnahmen im Rahmen der Erstellung einer IT-Sicherheitspolitik zu berücksichtigen sind. Bei der Bewertung besteht generell das Problem, dass der durch eine Schutzmaßnahme entstehende Aufwand und Schutz nicht einfach und zuverlässig bestimmt werden kann (vgl. Unterabschnitt 6.4.1 und Abschnitt 8.4). Bei den Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, gilt dies insbesondere für den durch die Einbeziehung entstehenden Aufwand, der sich z.B. durch Einbußen in der Produktivität äußern kann. Außer durch Problemen bei der Erfassung dieser Größen entstehen dadurch Schwierigkeiten, dass es Schutzmaßnahmen gibt, die nur im Zusammenhang mit anderen eine optimale Wirkung erzielen. In diesem Fall ist es nicht eindeutig, wie der entstehende Aufwand bzw. Nutzen den Schutzmaßnahmen zugerechnet werden muss.

Betrachtet man in den Tabellen 6.1 und 7.3 die Wirkungen der Schutzmaßnahmen, so kann festgestellt werden, dass diese generell nicht zueinander korrespondieren. Daher ist es im Rahmen einer Auswahl nicht einfach möglich, die Schutzmaßnahmen bzgl. ihrer Wirkung in Klassen von austauschbaren Schutzmaßnahmen zu unterteilen, die erlauben würden, für jede Klasse unabhängig von den anderen zu ermitteln, welche Schutzmaßnahme zu wählen ist. Stattdessen ist es bei der Auswahl der Schutzmaßnahmen notwendig, ein aufeinander abgestimmtes Gesamtkonzept zu verfolgen. Dabei ist zu beachten, dass bereits in den im Kapitel 4 aufgestellten Szenarien sowohl solche Vorfälle gezeigt wurden, denen nicht mit den in Kapitel 5 betrachteten Schutzmaßnahmen entgegengewirkt werden kann, als auch solche Vorfälle, denen nicht mit den hier betrachteten herkömmlichen Maßnahmen entgegengewirkt werden kann.

7.2.2 Implementierung, Bekanntmachung und Akzeptanz der gewählten Schutzmaßnahmen

Generell ist bei der Implementierung von Schutzmaßnahmen darauf zu achten, dass Möglichkeiten zur Umgehung soweit wie möglich vermieden und die Arbeitsabläufe der Nutzer durch den Einsatz der Schutzmaßnahmen so wenig wie möglich beeinflusst werden. Bei den herkömmlichen Schutzmaßnahmen entsteht durch die Implementierung oft fast ausschließlich Aufwand für die Administratoren. Bei den Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, entsteht während der Durchsetzung oft ein hoher Aufwand bei den Nutzern, der auch durch eine bei diesen Maßnahmen besonders wichtige Motivierung und Bekanntmachung zu begründen ist. Im Rahmen der Bekanntmachung entsteht u.a. Aufwand dadurch, dass diese vorbereitet und durchgeführt werden muss. Dies gilt insbesondere bei den in Kapitel 5 aufgezeigten Schutzmaßnahmen, bei denen im Allgemeinen

eine umfangreichere Bekanntmachung notwendig ist. Bei der Bekanntmachung ist insbesondere zu beachten, dass die Nutzer in der Zeit, die zur Bekanntmachung der Maßnahmen genutzt wird, der Erfüllung ihrer Aufgaben nicht nachkommen können. Insbesondere bei Maßnahmen, die eine Kooperation der Nutzer voraussetzen, ist bei den Nutzern eine hohe Akzeptanz für die Durchführung der Maßnahmen notwendig, die im Allgemeinen nur durch eine Motivierung der Nutzer erreicht werden kann (vgl. Abschnitt 8.1). Die Notwendigkeit einer Kooperation ist insbesondere bei den die Maßnahmen gegeben, bei denen eine Einbeziehung der Nutzer erfolgt.

7.2.3 Betrieb und Wartung der Schutzmaßnahmen

Bei den in Kapitel 5 aufgezeigten Schutzmaßnahmen entsteht teilweise auch beim Betrieb ein hoher Aufwand bei den Nutzern (vgl. Abschnitt 6.3). Bei den herkömmlichen Maßnahmen sollte im Idealfall kein zusätzlicher Aufwand entstehen. Es ist aber denkbar, dass durch diese Maßnahmen Möglichkeiten eingeschränkt werden, die die Arbeitsabläufe der Nutzer zwar vereinfachen, aber auch ein nicht akzeptables Risiko nach sich ziehen würden. Im Rahmen der Wartung ist es insbesondere bei den Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, notwendig, nicht nur technische Aspekte, sondern auch die mit der Einbeziehung der Nutzer zusammenhängenden Aspekte zu betrachten.

7.3 Zusammenfassung

In diesem Kapitel wurden zunächst im Abschnitt 7.1 die folgenden als herkömmlich betrachteten Schutzmaßnahmen eingeführt: „Firewalls“, Maßnahmen zur Kontrolle der Verwendung von Passworten, „Single Sign On“, Alternativen zur Authentisierung durch Wissen, „Intrusion Detection Systems“ und „Intrusion Response Systems“, „Antimalware“-Software, Redundante Auslegung von Diensten und Server, Kryptographische Verfahren und Physikalische Maßnahmen. Es wurde gezeigt, dass diese Schutzmaßnahmen einerseits nicht allen in den Szenarien aufgeführten Vorfällen entgegenwirken, andererseits aber auch Wirkungen haben, denen kein entsprechendes Szenario gegenüber steht. Als ein durch die Nutzer entstehendes Risiko wurde die mögliche Umgehung der Schutzmaßnahmen gesehen. Ferner wurde darauf hingewiesen, dass der Einsatz dieser Maßnahmen dazu führen kann, dass andere Vorsichtsmaßnahmen vernachlässigt werden. Bezüglich des durch die Schutzmaßnahmen entstehenden Aufwands konnte festgestellt werden, dass sie auf Seiten der Nutzer im Allgemeinen keinen oder nur wenig Aufwand erzeugen.

Beim im Abschnitt 7.2 erfolgten Vergleich zu den im Kapitel 5 aufgestellten Schutzmaßnahmen wurde gezeigt, dass es neben allgemeinen Problemen bei der Bewertung von Schutzmaßnahmen bei diesen zusätzlich das Problem gibt, dass der durch die Bekanntmachung und den Betrieb bei den Nutzern entstehende Aufwand schwer abgeschätzt werden kann. Dieser muss aber oft als hoch und insbesondere als höher als bei den herkömmlichen Schutzmaßnahmen angesehen werden.

Kapitel 8

Möglichkeiten zur Durchsetzung der Nutzer einbeziehenden Schutzmaßnahmen

- Ziel:
  Aufzeigen von Vorgehensweisen zur und Anforderungen an die Durchsetzung der in Kapitel 5 aufgezeigten Schutzmaßnahmen.
- Vorgehen:
  1. Betrachtung von Möglichkeiten zur Motivierung
  2. Betrachtung von Möglichkeiten zur Bekanntmachung
  3. Betrachtung von Anforderungen an die Implementierung
  4. Betrachtung von Möglichkeiten des „Controlling“
  5. Betrachtung der Schutzmaßnahmen

In diesem Kapitel sollen Möglichkeiten zur Durchsetzung der im Kapitel 5 aufgezeigten Schutzmaßnahmen betrachtet werden. Dazu sollen zunächst im Abschnitt 8.1 Möglichkeiten zur Motivierung der Nutzer aufgezeigt werden. Dann sollen im Abschnitt 8.2 Methoden zur Bekanntmachung wie Dokumente und Schulungen betrachtet werden. Dem folgend sollen im Abschnitt 8.3 die Nutzer betreffende Aspekte der Implementierung von Schutzmaßnahmen aufgezeigt werden. Im Abschnitt 8.4 sollen Möglichkeiten der Überprüfung der Wirkung der Schutzmaßnahmen („Controlling“) behandelt werden. Anschließend soll im Abschnitt 8.5 eine Betrachtung der im Kapitel 5 aufgezeigten Schutzmaßnahmen erfolgen. Im Abschnitt 8.6 soll eine Zusammenfassung dieses Kapitel abschließen.

8.1 Motivierung der Nutzer

In dieser Arbeit wurde bereits an verschiedenen Stellen darauf hingewiesen, dass zur Gewährleistung einer angemessenen Wirksamkeit der Schutzmaßnahmen auch eine kooperative Haltung der Nutzer notwendig ist (vgl. Unterabschnitt 3.2.2, Unterabschnitt 6.2.2, Abschnitt 6.3 und Unterabschnitt 7.2.2). Besteht diese kooperative Haltung bei den Nutzern nicht, steigt das Risiko, dass die Schutzmaßnahmen von ihnen umgangen werden. Dies kann oft darauf zurückgeführt werden, dass auf der einen Seite der Nutzen der Schutzmaßnahmen von den Nutzern nicht erkannt wird, auf der anderen Seite durch den Einsatz der Schutzmaßnahmen die Arbeitsabläufe der Nutzer mit mehr Aufwand verbunden sind bzw. diese an die Anforderungen der Schutzmaßnahmen angepasst werden müssen.

Um bei den Nutzern eine Motivierung zur kooperativen Mitarbeit bei den Schutzmaßnahmen zu erreichen, sollten diese von der Notwendigkeit des Einsatzes der Schutzmaßnahmen überzeugt werden. Dabei sollte ihnen nicht nur der Nutzen für die Organisation, sondern insbesondere auch der sie direkt betreffende Nutzen (z.B. Erhaltung des Arbeitsplatzes) aufgezeigt werden.

Um die Nutzer von der Notwendigkeit des Einsatzes der Schutzmaßnahmen zu überzeugen, ist es zunächst notwendig, ihnen aufzuzeigen, welche Probleme auftreten können, wenn keine oder unzureichende Schutzmaßnahmen eingesetzt bzw. die eingesetzten Schutzmaßnahmen umgangen werden. Dies sollte grundsätzlich nicht nur anhand von theoretischen Szenarien, sondern wenn möglich anhand von realen, u.U. in den Medien diskutierten Vorfällen erfolgen. Dadurch soll den Nutzern verdeutlicht werden, dass derartige Fälle in der Praxis tatsächlich auftreten und nicht nur imaginäre Beispiele darstellen. Nachdem der durch einen derartigen Vorfall entstehende Schaden veranschaulicht wurde, sollten die Auswirkungen des Einsatzes der Schutzmaßnahmen aufgezeigt werden. Die bei der Motivierung der Nutzer verwendeten Vorgehensweisen können sich an den im folgenden Abschnitt zu behandelnden Methoden zur Bekanntmachung orientieren.

8.2 Methoden zur Bekanntmachung

In diesem Abschnitt sollen Methoden zur Bekanntmachung betrachtet werden. Ziel dieser Methoden soll es sein, Wissen an die Nutzer zu vermitteln. Dies ist z.B. bei der Maßnahme „Bekanntmachung der Sicherheitspolitik“ (vgl. Abschnitt 8.5) relevant. Grundsätzlich soll hier die Bekanntmachung durch Dokumente (vgl. Unterabschnitt 8.2.1) und die Bekanntmachung durch Schulungen (vgl. Unterabschnitt 8.2.2) unterschieden werden.

8.2.1 Bekanntmachung durch Dokumente

In diesem Unterabschnitt soll betrachtet werden, in welcher Form Dokumente im Rahmen der Bekanntmachung eingesetzt werden können und wie sich der Einsatz verschiedener Typen von Dokumenten auf verschiedene Anforderungen bei der Bekanntmachung auswirken kann. Verschiedene Typen von Dokumenten können z.B. anhand ihres Umfangs und ihres

Grades der Detaillierung unterschieden werden. Im Folgenden sollen umfassende Handbücher, Richtlinien, Handlungsanweisungen und Sammlungen von sog. FAQs (Frequently Asked Questions) unterschieden werden. Dabei sollen sowohl gedruckte als auch elektronisch zur Verfügung gestellte Dokumente betrachtet werden. Bei der Betrachtung dieser Typen von Dokumenten soll insbesondere die Eignung für die folgenden Einsatzmöglichkeiten von Dokumenten bei der Bekanntmachung betrachtet werden:

- Die Dokumente werden zur Vermittlung neuen Wissens eingesetzt (z.B. bei der Bekanntmachung von Änderungen oder bei der Einweisung neuer Mitarbeiter).
- Die Dokumente werden zur Wiederholung bereits bekannt gemachten Wissens eingesetzt.
- Die Dokumente werden als Nachschlagewerk eingesetzt (z.B. zum Nachschlagen der vorgeschriebenen Vorgehensweise bei selten auftretenden Situationen).

Ferner soll betrachtet werden, inwieweit eine Motivierung der Nutzer beim Einsatz dieser Typen von Dokumenten möglich ist.

Umfassende Handbücher

Handbücher können sehr umfangreich sein und daher alle für einen bestimmten Bereich relevanten Informationen enthalten. Der abgedeckte Bereich kann die gesamte Organisation umfassen, insbesondere bei großen Organisationen aber auch nach Organisationseinheiten wie z.B. Abteilungen oder bestimmten Funktionen wie z.B. Sachbearbeiter und Abteilungsleiter abgegrenzt sein. Da es grundsätzlich keine Beschränkung beim Umfang der Handbücher gibt, können in diesen viele unterschiedliche Aspekte (z.B. Nutzung von Software und Verhalten bei eingehenden Telefonanrufen) sehr detailliert und ausführlich behandelt werden. Grundsätzlich setzt die Verwendung von Handbüchern Grundkenntnisse z.B. aus dem Bereich der Bedienung von IT-Systemen (Bedienung von Ein- und Ausgabemedien, Starten von Anwendungen u.Ä.) voraus.

Handbücher können sowohl in gedruckter Form vorliegen als auch elektronisch abrufbar sein. Liegen die Handbücher in gedruckter Form vor, muss geklärt werden, in welcher Anzahl sie verteilt werden sollen (z.B. ein Exemplar pro Mitarbeiter oder Abteilung). Gedruckte Fassungen haben insbesondere den Nachteil, dass Änderungen oder Fehlerkorrekturen nicht einfach eingebracht werden können. Elektronische Exemplare können zwar grundsätzlich auch aktuelle Sachverhalte widerspiegeln, dies gilt aber nur, wenn sie zentral abgerufen bzw. dezentrale Kopien regelmäßig aktualisiert werden. Im Allgemeinen besteht die Tendenz, dass insbesondere längere Texte nicht am Bildschirm gelesen, sondern ausgedruckt werden.

Um Änderungen und insbesondere geringfügige Änderungen bekannt zu machen, sind Handbücher generell nicht geeignet, da die Nutzer selbst bei einer besonderen Kennzeichnung der Änderungen das gesamte Handbuch nach diesen durchsuchen und sich selbst einen Überblick verschaffen müssten. Zur Einweisung neuer Mitarbeiter sind Handbücher

generell nur bedingt geeignet. Im Allgemeinen sind sie zu umfangreich und enthalten zu viele Details, als dass sie ganz gelesen, verstanden und behalten werden können. Es ist aber denkbar, dass sie in einer Weise gestaltet werden, dass einzelne Abschnitte die generellen Verhaltensweisen einführen, während in anderen Teilen speziellere Fragestellungen behandelt werden. Bei einer derartigen Gestaltung müssten neue Mitarbeiter zunächst nur die generellen Verhaltensweisen betrachten und erst bei Bedarf weitere spezielle Regelungen nachschlagen. Dabei bietet es sich an, dass im Rahmen der Abschnitte über die generellen Verhaltensweisen auch Aspekte zur Motivierung der Nutzer behandelt werden. Diese Abschnitte über die generellen Verhaltensweisen sollten von allen Mitarbeitern periodisch wiederholt werden. Werden Handbücher als Nachschlagewerk eingesetzt, in denen die vorgeschriebene Vorgehensweise im Zweifel nachgeschlagen werden kann (z.B. in Situationen, die nur selten oder bei neuen Mitarbeitern zum ersten Mal auftreten), muss darauf geachtet werden, dass der Aufbau des Dokuments diesem Zweck angemessen ist, die benötigten Regelungen also in angemessener Zeit gefunden werden können. Elektronische Dokumente erlauben dabei grundsätzlich sowohl einen Einsatz von Suchfunktionen zum gezielten Auffinden von Informationen als auch den Einsatz von Hypertext. Die beim Einsatz von Hypertext bestehende Möglichkeit, Verweise zwischen verschiedenen Teilen von Dokumenten einzurichten, kann ein besseres Nachschlagen ermöglichen und von Nutzern dazu genutzt werden, um zugehörige, ihnen bisher nicht bekannte Sachverhalte zu erlernen. Generell kann Hypertext aber auch schnell unübersichtlich werden („Lost in Cyberspace“).

Der Einsatz derartiger Handbücher birgt grundsätzlich verschiedene Probleme. Zunächst kann eine nicht angemessene Gestaltung die Handhabbarkeit der Handbücher einschränken. Ferner kann ihr Umfang auf Nutzer eine abschreckende Wirkung haben, die dazu führen kann, dass sie von diesen nicht verwendet werden. Schließlich sind die in den Handbüchern enthaltenen Informationen auch wertvoll für potentielle Angreifer, so dass der Zugriff auf die Handbücher eigentlich stark eingeschränkt werden müsste, was im Allgemeinen nicht praktikabel sein wird.

Richtlinien

Richtlinien stellen eine Zusammenfassung der in den Handbüchern behandelten Sachverhalte dar. Im Rahmen der Richtlinien werden keine Details ausgeführt, wodurch der Umfang deutlich geringerer ausfällt. Aufgrund des geringeren Detaillierungsgrades sind bei der Verwendung von Richtlinien deutlich mehr Vorkenntnisse als bei der Verwendung von Handbüchern notwendig. Richtlinien können ebenso wie Handbücher in gedruckter oder elektronischer Form vorliegen. Die mit der gewählten Form verbundenen Auswirkungen entsprechen grundsätzlich denen der Handbücher.

Um Änderungen bekannt zu machen, sind Richtlinien aus ähnlichen Gründen wie bei den Handbüchern oft nicht geeignet. Zur Einweisung von neuen Mitarbeitern sind Richtlinien aufgrund der vorausgesetzten Vorkenntnisse grundsätzlich nicht geeignet. Richtlinien können zum Nachschlagen genutzt werden, wenn eine hierfür angemessene Gliederung vorhanden ist. Dies kann z.B. dann sinnvoll sein, wenn Nutzern sowohl die generellen Vorgehensweisen als auch die Details der Durchführung einzelner Schritte bekannt sind, sie

sich aber über die Anwendbarkeit bestimmter Regelungen in einer speziellen Situation nicht im Klaren sind. Dies soll durch folgendes Beispiel verdeutlicht werden: Einem Nutzer ist bekannt, dass vertrauliche Daten laut der Sicherheitspolitik nur verschlüsselt übertragen werden dürfen. Ferner ist ihm bekannt, wie er Daten verschlüsselt übertragen kann. In einem speziellen Fall ist er sich aber nicht sicher, ob die zu übertragenden Daten als vertraulich anzusehen sind.

Richtlinien bieten generell keine Möglichkeiten für eine Motivierung der Nutzer, da eine Behandlung dessen oft ihrem knappen und zusammenfassenden Charakter widersprechen würde. Beim Einsatz von Richtlinien muss darauf geachtet werden, dass die notwendigen Voraussetzungen bei den Nutzern vorhanden sind. Andernfalls kann der Einsatz von Richtlinien zur fehlerhaften Ausführung von Arbeitsabläufen führen.

Handlungsanweisungen

Handlungsanweisungen sollen themenbezogen, also für die verschiedenen im Rahmen der Geschäftsprozesse durchzuführenden Arbeitsabläufe, in knapper Form die vorgeschriebenen Handlungsfolgen aufzeigen. Im Gegensatz zu Richtlinien, in denen die generellen Verhaltensweisen aufgeführt sind, werden bei Handlungsanweisungen für spezielle Arbeitsprozesse die durchzuführenden Handlungen gleich einem „Kochrezept“ aufgeführt. Da sie sehr knapp gehalten werden sollen, wird der Detaillierungsgrad geringer als bei Handbüchern sein. Daher sind auch bei der Verwendung von Handlungsanweisungen Vorkenntnisse notwendig.

Die themenbezogene Untergliederung ermöglicht grundsätzlich eine bedarfsgerechtere Verteilung der Dokumente, als es z.B. bei Handbüchern möglich ist. Damit Nutzer nur Handlungsanweisungen erhalten, die sie betreffen, und bei der Verteilung von aufeinander aufbauenden Handlungsanweisungen die Reihenfolge eingehalten wird (hierbei sind insbesondere Regelungen für neue Mitarbeiter zu treffen), ist eine Planung bei der Erstellung und Verteilung der Handlungsanweisungen notwendig. Dabei ist zu beachten, dass eine bei den Nutzern angesammelte, unsortierte Menge von einzelnen Handlungsanweisungen schnell unübersichtlich werden kann. Da das spätere Auffinden von bestimmten Handlungsanweisungen aus diesem Grund problematisch sein kann, ist diese Lösung zum Nachschlagen nur bedingt geeignet.

Um neues Wissen wie Änderungen zu vermitteln bzw. um bereits bekannt gemachtes Wissen zu wiederholen, können z.B. „Handlungsanweisung der Woche“ o.ä. eingeführt werden, bei denen jede Woche eine Handlungsanweisung verteilt und von den Nutzern gelesen wird. Es ist aber auch denkbar, dass auf aktuelle Ereignisse mit besonderen Notfall-Handlungsanweisungen eingegangen wird. Beide Varianten können insbesondere auch in elektronischer Form, z.B. durch Email oder durch ein sich beim Anmelden am IT-System öffnendes Fenster, durchgeführt werden. Im Fall eines sich öffnenden Fensters sollte unbedingt eine Möglichkeit vorgesehen werden, die es erlaubt, das Dokument später zu lesen, da Fälle auftreten können, in denen Nutzer in Eile sind, z.B. wenn sie kurz vor einer Besprechung noch schnell ihre Email überprüfen wollen. Hätten Nutzer in einem solchen Fall keine Möglichkeit, das Lesen des Dokuments zu verschieben, würden sie es wahrscheinlich gar nicht oder nur sehr oberflächlich lesen.

Das Problem, dass Nutzer periodisch verteilte Handlungsanweisungen nur oberflächlich oder gar nicht lesen, kann aber auch generell bestehen. Es kann insbesondere auftreten, wenn die Nutzer nicht erkennen, wie diese mit ihren Arbeitsabläufen zusammenhängen bzw. sie keinen Nutzen für sich sehen (vgl. Abschnitt 8.1). Eine Ursache hierfür kann sein, dass es im Rahmen der knapp zu haltenden Handlungsanweisungen nicht möglich ist, den Anwendungsbereich und den Nutzen der aufgezeigten Handlungsfolge angemessen darzustellen.

Sammlungen von FAQs

Der Einsatz von Sammlungen von FAQs (Frequently Asked Questions) kann erfolgen, um die konkreten Probleme der Nutzer besser berücksichtigen zu können. Dabei werden von Nutzern häufig gestellte Fragen und die Antworten auf diese Fragen gesammelt zur Verfügung gestellt. Ein großer Vorteil bei diesem Vorgehen ist, dass u.U. besser auf die Probleme eingegangen werden kann, die bei der alltäglichen Ausführung der Aufgaben entstehen und aufgrund von Ungenauigkeiten oder im schlimmsten Fall widersprüchlichen Angaben in den Regelungen nicht geklärt werden können. Eine Voraussetzung für die Erstellung derartiger Sammlungen ist, dass die Nutzer Möglichkeiten haben, ihre Fragen an zentraler Stelle zu stellen, und dass die gestellten Fragen entsprechend vermerkt und aufbereitet werden.

Sammlungen von FAQs können grundsätzlich in gedruckter oder in elektronischer Form vorliegen. Bei gedruckten Exemplaren sind die Möglichkeiten der Aktualisierung eingeschränkt. Bei elektronischen Exemplaren bestehen Möglichkeiten zur Aktualisierung nur, wenn auf das zentrale Exemplar zugegriffen wird bzw. dezentrale Kopien regelmäßig aktualisiert werden.

Für die Vermittlung von neuem Wissen sind Sammlungen von FAQs oft nicht geeignet, da der Auswahl der behandelten Fragen oft kein hierfür angemessenes Grundkonzept zugrunde liegt. Dies ergibt sich daraus, dass die Auswahl aus den alltäglichen Problemen erwächst und daher oft nur konkrete Probleme außerhalb ihres Gesamtkontexts behandelt werden. Für die Wiederholung bereits bekannten Wissens sind Sammlungen von FAQs nur bedingt geeignet, sie können aber die Möglichkeit bieten, bereits bekannte Themen aus einer anderen Sichtweise zu betrachten. Zum Nachschlagen sind Sammlungen von FAQs insbesondere dann geeignet, wenn der Gliederung der behandelten Fragen eine angemessene Strukturierung zugrunde liegt, so dass das Auffinden der relevanten Fragen in angemessener Zeit möglich ist. Grundsätzlich können in Sammlungen von FAQs auch Fragen behandelt werden, die auf den Nutzen der Regelungen eingehen und damit zur Motivierung der Nutzer beitragen können. Durch die Behandlung dieser Fragen kann insbesondere auch die Einstellung bzgl. derartiger Fragen beeinflusst werden, da ein Signal dafür gegeben wird, dass der Nutzen von Schutzmaßnahmen durch Nutzer hinterfragt werden darf.

8.2.2 Bekanntmachung durch Schulungen

Neben den Dokumenten stellen Schulungen eine weitere Möglichkeit zur Bekanntmachung dar. Bei der Durchführung von Schulungen ist eine Einbeziehung der Nutzer in verschiede-

nen Graden möglich. So können reine Vortragsveranstaltungen durchgeführt werden, bei denen eine Einbeziehung der Nutzer gar nicht oder nur durch die Möglichkeit des Stellens von Verständnisfragen gegeben ist. Ferner können Diskussionsveranstaltungen angeboten werden, bei denen die Nutzer nicht nur Verständnisfragen stellen, sondern z.B. auch die Angemessenheit und den Nutzen der Schutzmaßnahmen hinterfragen können. Das hierbei verfolgte Ziel kann z.B. sein, dass die Nutzer ein besseres Verständnis als bei reinen Vortragsveranstaltungen entwickeln. Schließlich ist es möglich, Veranstaltungen durchzuführen, in denen sich die Nutzer im Allgemeinen unter Anleitung der Veranstalter die Inhalte selbst erarbeiten sollen. Allgemein kann festgestellt werden, dass mit steigender Einbeziehung der Nutzer der Aufwand sowohl für die Vorbereitung durch die Veranstalter als auch für die zu schulenden Nutzer zunehmen wird. Auf der anderen Seite kann angenommen werden, dass insbesondere in Bezug auf die Motivation der Nutzer bessere Ergebnisse erzielt werden, wenn eine Einbeziehung dieser erfolgt (vgl. Unterabschnitt 3.2.2).

Schulungen können des Weiteren einerseits danach unterschieden werden, ob sie von Mitgliedern der Organisation oder von Externen durchgeführt werden, und andererseits, an welchen Orten sie durchgeführt werden. So ist es insbesondere bei kleinen Organisationen denkbar, dass die Schulungen, z.B. aufgrund von mangelnder Expertise innerhalb der Organisation oder aufgrund des nicht zu rechtfertigenden Aufwands, nicht von Mitgliedern der Organisation, sondern von Externen durchgeführt werden. Insbesondere in derartigen Fällen ist es oft auch denkbar, dass die Schulungen nicht innerhalb der Organisation stattfinden, so dass die Anreise zum Schulungsort als zusätzlicher Aufwand für die Nutzer berücksichtigt werden muss. Dabei kann grundsätzlich angenommen werden, dass bei Schulungen, die innerhalb der Organisation durchgeführt und von Mitgliedern der Organisation veranstaltet werden, im Allgemeinen eine angemessenere Berücksichtigung der aus der Umgebung entstehenden Anforderungen erfolgen wird. Auf der anderen Seite muss beachtet werden, dass Externe u.U. aufgrund einer größeren Erfahrung weniger Aufwand in die Vorbereitung investieren müssen und zusätzlich die Anforderungen und die Probleme der Nutzer besser einschätzen können. Grundsätzlich kann es sowohl sehr allgemeine Schulungen geben, bei denen keine Vorkenntnisse der Teilnehmer vorausgesetzt werden, als auch spezielle Schulungen zu bestimmten Themenbereichen, die Vorkenntnisse voraussetzen können.

8.2.3 Vergleich der Bekanntmachung durch Dokumente und Schulungen

Die Bekanntmachung durch Dokumente hat gegenüber der Bekanntmachung durch Schulungen den Vorteil, dass die Dokumente nach ihrer Erstellung ständig zur Verfügung stehen, so dass es den Nutzern z.B. möglich ist, bei Bedarf nachzulesen. Ein klarer Nachteil ist, dass es keine direkte Interaktion zwischen Verfasser und Leser gibt. Dadurch gestaltet es sich sowohl schwieriger, die Dokumente bedarfsgerecht, also in diesem Fall den Bedürfnissen der Nutzer entsprechend, zu gestalten als auch die bei vielen Schutzmaßnahmen als wichtig erachtete Motivierung der Nutzer zu erreichen.

Generell stellt sich bei der Bekanntmachung die Frage, wann und wie Sicherheitsfragen gelehrt werden sollen (vgl. [FH93]). Dabei ist zu klären, ob es besondere Maßnahmen zur Bekanntmachung von Aspekten aus dem Bereich der IT-Sicherheit, also z.B. zur Bekanntmachung der Sicherheitspolitik, geben soll oder ob diese Aspekte auch mit behandelt werden sollen, wenn eine Bekanntmachung genereller, mit den Aspekten der IT-Sicherheit im Zusammenhang stehender Aspekte erfolgt. Als Beispiele seien hier genannt, dass bei der Vorstellung von Unternehmenszielen auch die Ziele bzgl. der Sicherheit von IT-Systemen vorgestellt werden, und dass bei Einweisungen in die Nutzung von Anwendungssoftware immer eine Einweisung in die sichere Nutzung dieser Anwendungssoftware erfolgt. Insbesondere wenn es das Ziel einer Organisation ist, die Fragen der Sicherheit von IT-Systemen als integralen Bestandteil und nicht als zusätzliche Möglichkeit zu sehen, kann festgestellt werden, dass eine Behandlung der Fragen der Sicherheit im Rahmen aller Maßnahmen zur Bekanntmachung erfolgen sollte, in denen ein Zusammenhang besteht. Nur auf diese Weise wird es möglich sein, eine Nutzungskultur aufzubauen, in der die „sichere Nutzung von IT-Systemen“ die einzig denkbare ist.

8.3 Anforderungen an die Implementierung

In diesem Abschnitt sollen einige Aspekte betrachtet werden, die bei der Implementierung von Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, beachtet werden müssen. Diese Aspekte sind insbesondere bei der Durchsetzung der Schutzmaßnahmen „Durchsetzung der Pflichtentrennung“ und „Nutzer melden Sicherheitsvorfälle“ (vgl. Abschnitt 8.5) relevant. Dabei sollen sowohl Anforderungen betrachtet werden, die aus Sicht der Nutzer bestehen, als auch Anforderungen, die aus Sicht der das IT-System betreibenden Organisation bestehen.

Aus Sicht der Nutzer ist es zunächst wichtig, dass die Schutzmaßnahmen ihre Arbeitsabläufe so wenig wie möglich beeinträchtigen. Daher sollte der durch die Schutzmaßnahmen entstehende zusätzliche Aufwand möglichst gering gehalten werden. Es sollte aber auch dafür gesorgt werden, dass die Art und Weise, in der die Nutzer ihre Arbeitsabläufe ausführen, möglichst wenig durch die Schutzmaßnahmen bestimmt wird.

Aus Sicht der Organisation ist es wichtig, dass die Implementierung von Schutzmaßnahmen so durchgeführt wird, dass keine Beeinträchtigung der Wirksamkeit der Schutzmaßnahmen erfolgt. In Bezug auf die Nutzer sollten hier insbesondere potentielle Möglichkeiten zur Umgehung der Schutzmaßnahmen betrachtet werden. Gibt es technische Möglichkeiten, eine Umgehung zu erschweren, so sollten diese genutzt werden. Es ist aber zu beachten, dass durch derartige Maßnahmen unter Umständen eine Umgehung an anderer Stelle provoziert werden kann. Ein Beispiel hierfür wurde im Unterabschnitt 7.1.1 bei der Betrachtung der Maßnahmen zur Kontrolle der Verwendung von Passworten aufgezeigt: Wird die Verwendungsdauer von Passworten mit technischen Maßnahmen kontrolliert und die maximale Verwendungsdauer zu kurz angesetzt, kann als Folge das Risiko vergrößert werden, dass Nutzer ihre Passworte aufschreiben oder zyklisch wiederverwenden.

8.4 Kontrolle der Wirksamkeit („Controlling“)

In diesem Abschnitt soll die Kontrolle der Wirksamkeit der Schutzmaßnahmen betrachtet werden. Dazu soll zunächst aufzeigt werden, welche Probleme bei der Messung der Wirksamkeit von Schutzmaßnahmen auftreten können. Dann soll betrachtet werden, welche Probleme bei der Bewertung von Ergebnissen auftreten können.

Wie bereits im Unterabschnitt 6.4.1 angedeutet, ist es schwierig, die Wirksamkeit von Schutzmaßnahmen zu bestimmen. Zunächst ist es im Allgemeinen nicht möglich, festzustellen welche Vorfälle durch den Einsatz der Schutzmaßnahmen verhindert wurden und welche Schäden durch die nicht eingetretenen Vorfälle verursacht worden wären. Wird eine Bewertung aufgrund der trotz des Einsatzes der Schutzmaßnahmen eingetretenen Vorfälle durchgeführt, besteht insbesondere das Problem, eine angemessene Vergleichsmöglichkeit zu bestimmen. Dabei sind z.B. die folgenden Möglichkeiten denkbar (vgl. [KS98, Seite 454]):

- Der Zustand während des Einsatzes der Schutzmaßnahmen wird mit dem Zustand vor der Einführung verglichen.

- Der Zustand während des Einsatzes der Schutzmaßnahmen wird mit dem Zustand in anderen, ähnlichen Umgebungen verglichen.

- Die Schutzmaßnahmen werden nur in Teilen der Organisation eingeführt, um durch die übrigen Teile eine Vergleichsmöglichkeit zu haben.

Es kann allerdings festgestellt werden, dass alle hier aufgezeigten Möglichkeiten ihre Schwächen haben. Dies kann insbesondere darauf zurückgeführt werden, dass die äußeren Umstände bei den Vergleichsmöglichkeiten nicht exakt die gleichen wie die bei der Einsatzumgebung der Schutzmaßnahmen sein werden. Zum Beispiel können Unterschiede zwischen den Zuständen vor und nach der Einführung der Schutzmaßnahmen auch durch sich ändernde Bedrohungen und Verwundbarkeiten entstehen.

Die Bewertung der eingesetzten Schutzmaßnahmen in Bezug auf die durch neu auftretende Bedrohungen und Verwundbarkeiten entstehenden Risiken kann ebenfalls eine Aufgabe des „Controlling“ sein. Dabei müssen neue Bedrohungen und Verwundbarkeiten festgestellt und die Wirkung der bestehenden Schutzmaßnahmen gegen diese bewertet werden. Wird dabei festgestellt, dass die bestehenden Schutzmaßnahmen nicht ausreichen, um den neu entstandenen Risiken entgegenzuwirken, muss eine Anpassung der entsprechenden Teile der Sicherheitspolitik forciert werden.

8.5 Betrachtung der Schutzmaßnahmen

In diesem Abschnitt sollen die im Kapitel 5 aufgezeigten Schutzmaßnahmen in Bezug auf die in diesem Kapitel durchgeführten Betrachtungen zur Durchsetzung von Schutzmaßnahmen untersucht werden.

Bekanntmachung der Sicherheitspolitik

Nachdem eine Sicherheitspolitik erstellt wurde, müssen die für die Nutzer relevanten Teile diesen bekannt gemacht werden. Dazu ist es sinnvoll, bereits bei der Erstellung eine für die Nutzer angemessene Aufbereitung dieser Teile durchzuführen. In diesem Rahmen sollte insbesondere eine Darstellung des von den Nutzern erwarteten Verhaltens aufgeführt werden. Ferner sollte eine Motivierung der Nutzer erfolgen. Dabei sollte den Nutzern aufgezeigt werden, warum es notwendig ist, eine Sicherheitspolitik zu haben, und warum es notwendig ist, dass sich alle an die in der Sicherheitspolitik aufgestellten Regelungen halten.

Es bietet sich bei der Bekanntmachung der Sicherheitspolitik zunächst an, ein umfassendes Handbuch zur Verfügung zu stellen, in dem die gesamten für die Nutzer relevanten Aspekte der Sicherheitspolitik aufgeführt sind. Zusätzlich sollten Richtlinien zur Verfügung gestellt werden, die von Nutzern als eine Möglichkeit zum Nachschlagen genutzt werden können. Ferner kann es sinnvoll sein, periodische Handlungsanweisungen einzusetzen, um besonders zentrale und wichtige Punkte der Sicherheitspolitik den Nutzern regelmäßig in Erinnerung zu rufen. Außerdem können zur Bekanntmachung der Sicherheitspolitik Schulungen durchgeführt werden. Um den Aufwand hierbei in einen angemessenen Rahmen zu halten, können diese ebenso wie Handlungsanweisungen nur zur Behandlung besonderer Themen genutzt werden.

Um die Wirksamkeit der Bekanntmachung der Sicherheitspolitik zu überprüfen, können u.a. stichprobenhaft Befragungen von Nutzern durchgeführt werden. Dabei kann nicht nur überprüft werden, ob den Nutzern bestimmte Regelungen bekannt sind, sondern insbesondere auch, ob ihnen Zweck und Nutzen der Regelungen (die Motivation) bekannt ist.

Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen

Bei dieser Schutzmaßnahme soll den Nutzern Wissen über Angriffe vermittelt werden. Elementar ist es hierbei, den Nutzern zu vermitteln, welche Angriffe auftreten können und wie man diese erkennen kann. Dabei sollte aber möglichst wenig darauf eingegangen werden, wie diese im Detail durchgeführt werden, um zu verhindern, dass den Nutzern konkrete Anleitungen für die Durchführung von Angriffen gegeben werden. Hierbei bieten sich u.a. Schulungen an, bei denen z.B. auch die Durchführbarkeit von bestimmten Angriffen aufgezeigt werden kann (als Beispiel sei hier das Abhören von Passworten auf nicht verschlüsselten Verbindungen genannt). Ferner können periodische Handlungsanweisungen eingesetzt werden, mit denen z.B. auch auf aktuelle Bedrohungen hingewiesen werden kann.

Zur Überprüfung der Wirksamkeit können ebenso wie bei der Bekanntmachung der Sicherheitspolitik Befragungen eingesetzt werden. Ferner ist es denkbar, sog. „Penetration Tests“ durchzuführen, bei denen versucht wird, durch legitimierte Angriffe auf das IT-System Schwachstellen aufzudecken. Wird die Durchführung von „Penetration Tests“ in Erwägung gezogen, sollten die Nutzer im Voraus über die Möglichkeit informiert werden, dass derartige Tests ohne vorherige Ankündigung durchgeführt werden können, da es sonst zu Problemen im Verhältnis zwischen der Organisation und den Nutzern kommen kann.

Vorbeugung von Angriffen durch Nutzer

Eine Vorbeugung soll hier dadurch geschehen, dass den Nutzern der durch Angriffe entstehende Schaden bewusst gemacht wird. Hierbei ist insbesondere eine angemessene Motivierung der Nutzer notwendig, um einerseits zu verhindern, dass sich Nutzer pauschal als Angreifer verurteilt fühlen, und andererseits eine positive Grundstimmung gegenüber dieser Schutzmaßnahme zu erreichen. Dies kann z.B. im Rahmen von Schulungen durchgeführt werden. Dabei ist es möglich, die Nutzer z.B. anhand von realen Fallbeispielen über das Ausmaß von durch Angriffen verursachten Schäden und von möglichen Auswirkungen dieser Schäden in Kenntnis zu setzen.

Eine Überprüfung der Wirksamkeit dieser Schutzmaßnahme kann als schwierig angenommen werden. Insbesondere ist es in diesem Fall nicht sinnvoll, Befragungen durchzuführen, da Nutzer es kaum zugeben werden, wenn sie potentiell bereit wären, die Organisation bzw. das IT-System der Organisation anzugreifen.

Nutzer werden verantwortlich gemacht

Bei dieser Schutzmaßnahme muss insbesondere bekannt gemacht werden, in welchen Fällen die Nutzer verantwortlich gemacht und welche Sanktionen in diesen Fällen ergriffen werden. Besonders wichtig ist auch bei dieser Schutzmaßnahme eine Motivierung der Nutzer, indem sie von dem Nutzen der Durchsetzung von Sanktionen überzeugt werden.

Die Wirksamkeit dieser Schutzmaßnahme kann z.B. durch eine Beobachtung der Anzahl der durch Nutzer verursachten, mit Sanktionen belegten Vorfälle erfolgen. Wie bereits angemerkt, kann das Problem bestehen, dass die Anzahl dieser Vorfälle auch durch andere Bedingungen beeinflusst werden. Ferner wäre es notwendig, schon vor der Einführung dieser Schutzmaßnahme Zahlen über derartige Vorfälle zu erheben, um einen Vergleich überhaupt zu erlauben.

Durchsetzung der Pflichtentrennung

Insbesondere wenn zur Durchsetzung der Pflichtentrennung die Arbeitsabläufe und im Extremfall sogar die Organisationsstrukturen angepasst werden müssen, kann bei der Durchsetzung dieser Schutzmaßnahme ein hoher Aufwand entstehen. Dabei muss insbesondere bekannt gemacht werden, wie die Arbeitsabläufe gestaltet werden sollen. Ferner muss eine Motivierung der Nutzer erfolgen, um einer Umgehung der Pflichtentrennung, z.B. durch Weitergabe von Passworten, entgegenzuwirken. Um Missbrauch entgegenzuwirken, muss das Prinzip der geringsten Privilegien auf technischer Ebene durchgesetzt werden. Dabei ist zu beachten, dass die Vergabe der Privilegien nicht zu restriktiv gehandhabt wird, da dies eine Umgehung der Schutzmaßnahme provozieren könnte.

Nutzer melden Sicherheitsvorfälle

Bei dieser Schutzmaßnahme muss den Nutzern bekannt gemacht werden, was erreicht werden soll und wie der Ablauf gestaltet ist. Dabei muss insbesondere bekannt gemacht wer-

den, welches Verhalten von den Nutzern erwartet wird, also was sie melden sollen, wann sie es melden sollen, auf welche Weise eine Meldung erfolgt und was nach einer Meldung erfolgt. Ferner muss eine für diese Schutzmaßnahme notwendige Infrastruktur aufgebaut werden. Zum Beispiel ist es notwendig, Stellen einzurichten, an die die Meldungen der Nutzer gerichtet werden. Hier müssen die Meldungen aufgenommen, ähnliche Meldungen zusammengefasst und die Ursache für die der Meldung zugrunde liegende Beobachtung gefunden werden.

8.6 Zusammenfassung

In diesem Kapitel wurden Möglichkeiten zur Durchsetzung der Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, betrachtet. Dazu wurde zunächst im Abschnitt 8.1 aufgezeigt, dass eine Motivation der Nutzer vorhanden sein muss und z.B. durch die Betrachtung der Wirkung der Schutzmaßnahmen anhand von realen Szenarien erreicht werden kann. Im Abschnitt 8.2 wurden dann als verschiedene Methoden zur Bekanntmachung Dokumente und Schulungen betrachtet. Als Dokumente wurden umfassende Handbücher, Richtlinien, spezielle Handlungsanweisungen und Sammlungen von FAQs unterschieden. Bei den Schulungen wurde aufgezeigt, dass verschiedene Grade der Einbeziehung der Nutzer möglich sind und ein höherer Grad der Einbeziehung grundsätzlich zu mehr Aufwand, aber im Allgemeinen auch zu einem besseren Verständnis der Nutzer führen kann. Im Vergleich kann festgestellt werden, dass Dokumente den Vorteil haben, dass sie den Nutzern ständig zur Verfügung stehen und daher insbesondere zum Nachschlagen genutzt werden können, während bei Schulungen der Vorteil der Möglichkeit der Interaktion mit den Nutzern besteht. Als Anforderung an die Implementierung wurde im Abschnitt 8.3 aus Sicht der Nutzer eine möglichst geringe Auswirkung auf die Arbeitsabläufe und aus Sicht der Organisation eine möglichst geringe Beeinträchtigung der Wirksamkeit der Schutzmaßnahmen z.B. durch Möglichkeiten der Umgehung aufgeführt. Im Abschnitt 8.4 wurde gezeigt, dass es bei der Kontrolle der Wirksamkeit der Schutzmaßnahmen grundsätzlich das Problem gibt, dass die Wirkung von Schutzmaßnahmen nur schwer abgeschätzt werden kann und dass es weiterhin schwierig ist, einen angemessenen Vergleichsmaßstab zu ermitteln. Ferner wurde die Bewertung von neuen Verwundbarkeiten und Bedrohungen als Aufgabe des „Controlling“ identifiziert. Abschließend wurde im Abschnitt 8.5 für die im Kapitel 5 betrachteten Schutzmaßnahmen aufgezeigt, worauf bei der Durchsetzung geachtet werden muss und mit welchen Methoden eine Durchsetzung durchgeführt werden kann.

Kapitel 9

Zusammenfassung und Ausblick

In diesem Kapitel sollen zunächst die in dieser Arbeit aufgezeigten Ergebnisse zusammengefasst werden (vgl. Abschnitt 9.1). Dann soll ein Ausblick auf Fragestellungen gegeben werden, die sich bei der Ausarbeitung ergeben haben, im Rahmen dieser Diplomarbeit aber nicht behandelt werden konnten (vgl. Abschnitt 9.2).

9.1 Zusammenfassung der Ergebnisse

In dieser Arbeit sollte betrachtet werden, auf welche Weise eine Einbeziehung der Nutzer bei der Erstellung und Durchsetzung einer Sicherheitspolitik durchgeführt werden kann und welche Auswirkungen sich daraus ergeben können. Dazu wurde zunächst im Rahmen einer Einführung und Abgrenzung von verwendeten Begriffen eine Abgrenzung des Begriffs Nutzers durchgeführt, bei der aufgezeigt wurde, dass als Nutzer solche Personen verstanden werden sollen, die ein IT-System zur Erfüllung ihrer Aufgaben nutzen und bei denen die Gewährleistung des Betriebs des IT-Systems nicht Teil ihrer Aufgaben ist. In Bezug auf die Einbeziehung der Nutzer bei der Erstellung einer Sicherheitspolitik wurde festgestellt, dass es keinen allgemein gültigen Schluss über eine optimale Art der Einbeziehung gibt. Generell kann aber gesagt werden, dass auf der einen Seite eine breitere Einbeziehung der Nutzer zu einem höheren Aufwand führt, auf der anderen Seite eine Einbeziehung der Nutzer zu Vorteilen bei der Durchsetzbarkeit und der Wirksamkeit der zu erstellenden Sicherheitspolitik führen kann.

Um die Möglichkeiten der Einbeziehung der Nutzer bei der Durchsetzung einer Sicherheitspolitik zu betrachten, wurden einige Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, aufgezeigt und im Hinblick auf ihre Wirkung, die mit ihrem Einsatz verbundenen Risiken und den durch den Einsatz der Schutzmaßnahmen entstehenden Aufwand untersucht und mit herkömmlichen Schutzmaßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, verglichen. Um die Wirkung dieser Schutzmaßnahmen zu beurteilen, wurden die Auswirkungen auf dreizehn, im Rahmen von Szenarien aufgezeigten Vorfällen betrachtet, in denen Nutzer als eine Verwundbarkeit des IT-Systems, als eine Bedrohung für das IT-System oder als Beobachter eines Vorfalls auftraten. Um die Risiken zu unter-

suchen, wurden Möglichkeiten zur Einschränkung der Wirksamkeit durch Fehler bei der Durchsetzung, Möglichkeiten und Ursachen für eine Umgehung durch die Nutzer und mit dem Einsatz der Schutzmaßnahmen evtl. einhergehende Seiteneffekte betrachtet. Bei der Betrachtung des Aufwands wurde der durch die Durchsetzung, durch die Wartung und durch den Betrieb der Schutzmaßnahmen entstehende Aufwand aufgezeigt.

Es wurde gezeigt, dass die „Bekanntmachung der Sicherheitspolitik“ oft eine Voraussetzung für weitere Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, ist. Ferner wurde gezeigt, dass es sinnvoll sein kann, eine „Entwicklung eines Verständnisses für Hintergründe, Ziele, Vorgehensweisen und Erkennungsmerkmale von Angriffen“ durchzuführen. Dies gilt insbesondere, wenn die Schutzmaßnahme „Nutzer melden Sicherheitsvorfälle“ eingesetzt werden soll, deren Wirksamkeit durch ein besseres Verständnis der Nutzer deutlich verbessert wird. Bezüglich der „Durchsetzung der Pflichtentrennung“ wurde zunächst gezeigt, dass sie insbesondere in kleinen Organisationen u.U. nicht sinnvoll umgesetzt werden kann. Um bei der Einführung dieser Schutzmaßnahme einen hohen Aufwand durch die Umstrukturierung der Geschäftsprozesse zu vermeiden, sollten diese eine Pflichtentrennung bereits möglichst weit durchsetzen. Bei der Betrachtung der Schutzmaßnahme „Nutzer werden verantwortlich gemacht“ wurde gezeigt, dass die Übernahme einer umfassenden Verantwortung durch die Nutzer nicht sinnvoll ist und daher immer Sache des Managements bleiben sollte. Schließlich wurde gezeigt, dass eine Einbeziehung der Nutzer bei der „Vorbeugung von Angriffen durch Nutzer“ im Allgemeinen nicht sinnvoll ist, da sie oft einen im Verhältnis zum erwarteten Nutzen zu hohen Aufwand nach sich ziehen wird und außerdem eine Störung des Verhältnisses zwischen der Organisation und den Nutzern auftreten kann, wenn sich diese pauschal verurteilt fühlen.

Beim Vergleich mit herkömmlichen Schutzmaßnahmen, bei denen keine Einbeziehung der Nutzer erfolgt, konnte zunächst sowohl bei den Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, als auch bei den herkömmlichen Schutzmaßnahmen festgestellt werden, dass es Vorfälle gibt, gegen die diese keine Wirkung zeigen. Der Einsatz von Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, kann daher nicht als eine Alternative, sondern immer nur als eine Ergänzung zum Einsatz von herkömmlichen Schutzmaßnahmen gesehen werden. Ferner konnte festgestellt werden, dass der Aufwand, der durch eine Einbeziehung bei den Schutzmaßnahmen für die Nutzer entsteht, insbesondere bei der Durchsetzung, aber oft auch beim Betrieb der Schutzmaßnahmen deutlich höher als beim Einsatz von herkömmlichen Schutzmaßnahmen sein wird.

Während dieser Betrachtungen wurde mehrfach auf die Wichtigkeit einer Motivierung der Nutzer hingewiesen. Es wurde gezeigt, dass eine Motivation der Nutzer erreicht werden kann, indem diese von der Notwendigkeit der Durchführung der Schutzmaßnahmen überzeugt werden.

Als Möglichkeiten zur Durchführung einer Bekanntmachung, die im Rahmen der Durchsetzung von Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, notwendig ist, wurde die Verwendung von Schulungen und verschiedenen Arten von Dokumenten betrachtet. Schließlich wurde gezeigt, dass eine Kontrolle der Wirksamkeit von Schutzmaßnahmen oft schwierig ist, da die hierfür notwendigen Größen im Allgemeinen nur abgeschätzt werden können und ein angemessener Vergleichsmaßstab oft nicht gegeben ist.

Als Fazit kann festgestellt werden, dass es dann sinnvoll ist, die Nutzer bei der Erstellung und Durchsetzung einer Sicherheitspolitik einzubeziehen, wenn es gelingt, diese hierfür zu motivieren.

9.2 Ausblick und offene Fragen

Bei der Erstellung dieser Arbeit ergaben sich verschiedene Fragestellungen, die im Rahmen der Arbeit nicht behandelt werden konnten. Diese würden die in dieser Arbeit durchgeführten Betrachtungen weiterführen.

Möglichkeiten der Ausgestaltung der Schutzmaßnahmen

Die betrachteten, die Nutzer einbeziehenden Schutzmaßnahmen wurden im Rahmen dieser Arbeit nur sehr abstrakt beschrieben. An dieser Stelle könnte eine Betrachtung der Möglichkeiten der Ausgestaltung dieser Schutzmaßnahmen in verschiedenen Einsatzumgebungen durchgeführt werden. Dabei könnte insbesondere ergänzt werden, in welchen Einsatzumgebungen der Einsatz der verschiedenen Schutzmaßnahmen sinnvoll bzw. nicht sinnvoll ist.

Motivierung der Nutzer

Bezüglich der Möglichkeiten der Motivierung von Nutzern besteht ebenfalls die Möglichkeit detailliertere Betrachtungen durchzuführen.

Auswirkungen des Einsatzes von Schutzmaßnahmen auf die Arbeitsabläufe der Nutzer

Schließlich könnte sowohl für Schutzmaßnahmen, bei denen eine Einbeziehung der Nutzer erfolgt, als auch für Schutzmaßnahmen, bei denen keine Einbeziehung erfolgt, näher untersucht werden, wie sich der Einsatz der Schutzmaßnahmen auf die Arbeitsabläufe der Nutzer auswirkt. Dabei könnte insbesondere betrachtet werden, wie viel zusätzlicher Aufwand für die Nutzer entsteht und worauf dieser zusätzliche Aufwand im Einzelnen zurückgeführt werden kann.

Literaturverzeichnis

[AS99] Adams, Anne and Martina Angela Sasse: *Users are not the enemy — why users compromise computer security mechanisms and how to take remedial measures*. Communications of the ACM, 42(12):41 – 46, December 1999.

[BFH92] Brunnstein, Klaus und Simone Fischer-Hübner: *Möglichkeiten und Grenzen von Kriterienkatalogen*. Wirtschaftsinformatik, 34(4):391 – 400, August 1992.

[Bru93] Brunnstein, Klaus: *I.T. Paradigms and Inherent Risks*. In Berleur, J., C. Beardon, and R. Laufer (editors): *Facing the Challenge of Risk and Vulnerability in an Information Society*, Proceedings of the IFIP WG9.2 Working Conference, pages 77–88, Amsterdam, 1993. IFIP, Elsevier Science Publishers B.V. (North-Holland).

[Bru02] Brunnstein, Klaus: *Beherrschbarkeit von zukünftigen sicheren IT-Systemen: Anforderung an Planung, Implementierung und Betrieb*. In: *Eingeladener Vortrag 7. Kongress Software-Qualitätsmanagement (SQM)*, Düsseldorf, 19. April 2002.

[BSI01] BSI, Bundesamt für die Sicherheit in der Informationstechnik: *IT-Grundschutzhandbuch*, Juli 2001. `www.bsi.de/gshb/`.

[CC999] *Common criteria for information technology security evaluation*, August 1999. `http://commoncriteria.org/`.

[CER99] CERT/CC, Computer Emergency Response Team Coordination Center: *CERT Advisory CA-1999-04 Melissa Macro Virus*, March 1999. `http://www.cert.org/advisories/`.

[CER00] CERT/CC, Computer Emergency Response Team Coordination Center: *CERT Advisory CA-2000-04 Love Letter Worm*, May 2000. `http://www.cert.org/advisories/`.

[CER01] CERT/CC, Computer Emergency Response Team Coordination Center: *CERT Advisory CA-2001-03 VBS/OnTheFly (Anna Kournikova) Malicious Code*, February 2001. `http://www.cert.org/advisories/`.

[CW87] Clark, David D. and David R. Wilson: *A comparison of commercial and military computer security policies.* In *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, pages 184–194, Oakland, CA, USA, 27-29 April 1987. IEEE, IEEE Computer Society Press.

[CZ95] Chapman, D. Brent and Elizabeth D. Zwicky: *Building Internet Firewalls.* O'Reilly & Associates, Inc., first edition, 1995.

[DoD85] DoD, US Department of Defense: *Department of defense trusted computer system evaluation criteria*, 26. December 1985. DoD 5200.28-STD.

[Eck01] Eckert, Claudia: *IT-Sicherheit: Konzepte – Verfahren – Protokolle.* Oldenbourg Verlag, München, 2001.

[Ell99] Ellermann, Uwe: *Firewalls in Hochgeschwindigkeitsnetzen.* Doktorarbeit, Fachbereich Informatik, Universität Hamburg, 1999.

[FH93] Fåk, Viiveke and Amund Hunstad: *Teaching security basics: The importance of when and how.* In Dougall, E.G. (editor): *Computer Security (A-37)*, pages 23 – 30. IFIP, Elsevier Science Publishers B.V. (North-Holland), 1993.

[FKB89] Fites, Philip E., Martin P. J. Kratz, and Alan F. Brebner: *Control and Security of Computer Information Systems.* Computer Science Press, Rockville, 1989.

[Fra97] Fraser, B.: *Site Security Handbook*, September 1997. RFC 1244.

[Gel00] Gellert, Olaf: *Sicherheitsdienste im TCP/IP-Protokollstapel.* Diplomarbeit, Fachbereich Informatik, Universität Hamburg, Juni 2000.

[GG00] Gellert, Olaf und Gregor Goldbach: *httpf — Ein filternder Proxy.* In: *7. DFN Workshop Sicherheit in vernetzten Systemen*, Hamburg, März 2000.

[Gor95] Gordon, Sarah: *Social engineering: Techniques and prevention.* In *Proceedings of Compsec International 1995*, pages 445 – 450, Oxford, Oktober 1995. Elsevier.

[Gre96] Greening, Tony: *Ask and ye shall receive: A study in 'social engineering'.* ACM SIG Security, Audit & Control, 14(2):8 – 14, April 1996.

[Gro99] Grossklaus, Axel: *Policy, Vorfallsbearbeitung, Schwachstellenanalyse.* In: Mück, Hans-Joachim, Carsten Benecke und Stefan Kelm (Herausgeber): *Sicherheit in vernetzten Systemen*, Berichte des Fachbereichs Informatik (Bericht 224), Kapitel 4, Seiten 53–68. Fachbereich Informatik, Universität Hamburg, 1999.

[Hig93] Highland, Harold Joseph: *A view of information security tomorrow.* In Dougall, E.G. (editor): *Computer Security: Proceedings of the IFIP TC11 Ninth International Conference on Information Security*, IFIP transactions: A, Computer Science and technologie, 37, pages 1 – 11, Amsterdam, May 1993. IFIP, North Holland.

[Hol02] Holst, Stephan: *Absicherung von Netzdiensten am Beispiel des ATMARP-Dienstes.* Diplomarbeit, Fachbereich Informatik, Universität Hamburg, 2002.

[Irr01] Irrgang, Hartmut: *Erkennung von Einbrüchen in Netzwerke.* Diplomarbeit, Fachbereich Informatik, Universität Hamburg, August 2001.

[ITS91] *Information Technology Security Evaluation Criteria (ITSEC)*, June 1991.

[Ker95a] Kerner, Helmut: *Rechnernetze nach OSI.* Addison-Wesley, Bonn, 3. Auflage, 1995.

[Ker95b] Kersten, Heinrich: *Sicherheit in der Informationstechnik — Einführung in Probleme, Konzepte und Lösungen.* R. Oldenbourg Verlag, München Wien, 2. Auflage, 1995.

[Kos00] Kossakowski, Klaus-Peter: *Information Technology Incident Response Capabilities.* Doktorarbeit, Universität Hamburg, 2000.

[Kro01] Krooss, Michael: *Beurteilungskriterien für eine IP-über-ATM-Infrastruktur.* Studienarbeit, Fachbereich Informatik, Universität Hamburg, November 2001.

[Kro02] Kronberg, Marcel: *Implementierung einer Iris-Biometrik in ein „Client-Server-Authentisierungssystem“.* Diplomarbeit, Fachbereich Informatik, Universität Hamburg, Juni 2002.

[KS98] Kajava, Jorma and Mikko T. Siponen: *On the information security management in industry — IT security awareness perspective.* In Buch, N. J., J. Damsgaard, L. B. Eriksen, J. H. Iversen, and P. A. Nielsen (editors): *Proceedings of IRIS 21*, pages 447 – 456. Department of Computer Science, Aalborg University, 1998.

[Lal01] Lala, Parag K.: *Self-Checking and Fault-Tolerant Digital Design.* Morgan Kaufmann Publishers, San Francisco, 2001.

[Ned99] Nedon, Jens: *Ein IT-Sicherheitskonzept für eine wissenschaftliche Einrichtung.* Diplomarbeit, Fachbereich Informatik, Universität Hamburg, September 1999.

[Øln94] Ølnes, Jon: *Development of security policies.* Computers & Security, 13(8):628–636, 1994.

[Opp97] Oppliger, Rolf: *IT-Sicherheit – Grundlagen und Umsetzung in der Praxis*. DUD-Fachbeiträge. Vieweg, Braunschweig/Wiesbaden, 1997.

[Pfl96] Pfleeger, Charles P.: *Security in Computing*. Prentice Hall, Upper Saddle River, NJ, second edition, 1996.

[Sch98] Schuppenhauer, Rainer: *Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV); Handbuch der DV-Revision*. IDW-Verlag, Düsseldorf, 5. Auflage, 1998.

[Sch99] Schreyögg, Georg: *Organisation – Grundlagen moderner Organisationsgestaltung*. Gabler, Wiesbaden, 3. Auflage, 1999.

[Sta98] Stallings, William: *Cryptography and network security: principles and practice*. Prentice Hall, New Jersey, second edition, 1998.

[Ste91] Sterne, Danial F.: *On the buzzword "security policy"*. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pages 219–230, Los Alamitos, May 1991. IEEE, IEEE Computer Society Press.