



# Diplomarbeit

## IT-Sicherheits-Überprüfungen

*vorgelegt von*

Konstantin Bauer

Katzelsdorf/Leitha

*geboren am:* 02.03.1981

*Matr.-Nr.:* TM0010038004

Fachhochschule St. Pölten

FB Kommunikationsnetze und -dienste, Studiengang Telekommunikation und Medien

**Sommersemester 2004**

*Erstbegutachter:* Dipl.-HTL-Ing. Andreas Schaupp MSc

*Zweitbegutachter:* FH Prof. Dipl.-Ing. Johann Haag

## **Ehrenwörtliche Erklärung**

Ich erkläre hiermit an Eides Statt,

- dass ich die vorliegende Diplomarbeit selbstständig angefertigt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter beurteilten Arbeit überein

Katzelsdorf/Leitha, 23. Juni 2005

Konstantin Bauer

## Zusammenfassung

Die Sicherheit von IT-Infrastrukturen und Netzwerken nimmt einen immer größeren Stellenwert ein. Im Zuge dieser Entwicklung wird es notwendig zu prüfen, wie es um die IT-Sicherheit bestellt ist. Diese Diplomarbeit behandelt die Methodiken, Methoden und Werkzeuge, mit deren Hilfe die IT-Sicherheit einer Netzwerkinstallation überprüft werden kann. Darüber hinaus wird untersucht, wie diese in Österreich angeboten werden.

Zu Beginn der Arbeit wird auf die Wichtigkeit eines IT-Sicherheitsmanagement-Prozesses eingegangen. Es gibt verschiedene Gründe, die ein umfassendes IT-Sicherheitsmanagement notwendig machen, beispielsweise rechtliche Vorgaben oder das Risiko, welches Bedrohungen auf den Unternehmenswert IT ausüben. Ein wichtiger Bestandteil eines IT-Sicherheitsmanagement-Prozesses ist daher die IT-Sicherheits-Überprüfung, welche das gesamte IT-Sicherheitsmanagement auf seine Funktion überprüfen muss.

Der zweite Teil dieser Diplomarbeit widmet sich der genauen Beschreibung dreier verbreiteter umfassender Methodiken zur Überprüfung der IT-Sicherheit. Im Anschluss daran werden weitere Methodiken vorgestellt und anhand von Vergleichskriterien einander gegenübergestellt, um die jeweiligen Vor- und Nachteile aufzudecken.

Kapitel 3 der vorliegenden Arbeit beschreibt die Methoden und Werkzeuge, welche bei einer IT-Sicherheits-Überprüfung zur Erfüllung von Teilaufgaben zum Einsatz kommen. Nach der Beschreibung der Methoden wird eine Auswahl unterstützender Softwarewerkzeuge vorgestellt und anhand von Beispielen erläutert.

In Kapitel 4 wird der österreichische Markt für IT-Sicherheits-Überprüfungen charakterisiert und untersucht. Zu diesem Zweck kam ein Fragebogen zum Einsatz, der sich an die Anbieterelementsprechender Dienstleistungen wendete. Die Auswertung der Antworten auf den Fragebogen ist der letzte Schwerpunkt der Diplomarbeit. An der Auswertung wird erkennbar, welche Stärken und Schwächen das differenzierte Dienstleistungsangebot in Österreich aufweist, und welche Potentiale bei einem Ausbau des Marktes zur Verfügung stehen.

## **Abstract**

Since the security of IT infrastructures and networks is becoming more and more important these days, it is crucial to carry out IT security assessments. This diploma thesis covers the comprehensive approaches, methods and tools with which the IT security of network installations can be assessed. Furthermore, it examines the way they are offered by service companies in Austria.

Starting the thesis is a description of the importance and form of an IT security management process. There are multiple reasons which make a complete IT security management necessary, for instance laws or the risk, which is caused by threats to the IT asset. A major component of the IT security management process is therefore the IT security assessment, which has to assess the function of the IT security management in its whole.

The second part of this diploma thesis is devoted to the description of three widely used comprehensive IT security assessment approaches. In addition, further approaches are presented and compared to the previous ones to spot their advantages and disadvantages, respectively.

Chapter 3 of this diploma thesis describes the methods and tools, which are used during parts of an IT security assessment. After the description of the methods, a collection of supporting software tools is presented and described using common examples.

Chapter 4 examines and characterises the Austrian market for IT security assessments. For this purpose, a questionnaire was sent to companies offering this service. The Evaluation of the questionnaires is the diploma thesis' last emphasis. It reveals the Austrian service market's strengths and weaknesses and the potentials available for an extension of the service market.

## Inhaltsverzeichnis

Diplomarbeit.....	II
<b>Ehrenwörtliche Erklärung .....</b>	<b>III</b>
<b>Zusammenfassung.....</b>	<b>IV</b>
<b>Abstract .....</b>	<b>V</b>
<b>Inhaltsverzeichnis .....</b>	<b>VI</b>
<b>Einleitung .....</b>	<b>9</b>
<b>1 IT-Sicherheitsmanagement und IT-Sicherheits-Überprüfungen . 10</b>	
1.1 Problemstellung: Die Suche nach der „idealen“ IT-Sicherheits-Überprüfung .....	10
1.2 Forschungsleitende Fragestellung.....	10
1.3 Forschungsstrategie.....	10
1.4 Gründe für die Etablierung eines IT-Sicherheitsmanagement-Prozesses .....	11
1.5 Der IT-Sicherheitsmanagementprozess .....	14
1.5.1 Entwicklung einer organisationsweiten IT-Sicherheitspolitik.....	17
1.5.2 Risikoanalyse .....	18
1.5.3 Erstellung von IT-Sicherheitskonzepten .....	24
1.5.4 Umsetzung des IT-Sicherheitsplanes.....	28
1.5.5 IT-Sicherheit im laufenden Betrieb .....	29
1.6 Überlegungen zur Durchführung einer IT-Sicherheits-Überprüfung .....	32
1.7 Schlussfolgerungen .....	33
<b>2 Die Methodiken zur IT-Sicherheits-Überprüfung.....</b>	<b>34</b>
2.1 BSI Grundschutz .....	34
2.1.1 Anwendungsweisen des IT-Grundschutzhandbuchs .....	35
2.1.2 Die IT-Grundschutzmethode und ihre Anwendung .....	38
2.1.3 Laufende Entwicklungen des IT-Grundschatzes.....	56
2.1.4 Zertifizierung nach BSI Grundschutz.....	56
2.2 Operationally Critical Threat, Asset, and Vulnerability Evaluation <sup>SM</sup> - OCTAVE <sup>SM</sup> .....	57
2.2.1 Der OCTAVE <sup>SM</sup> -Ansatz .....	58
2.2.2 Die OCTAVE <sup>SM</sup> -Methode .....	63
2.2.3 Variationen des OCTAVE <sup>SM</sup> -Ansatzes .....	85
2.2.4 Laufende Entwicklungen von OCTAVE <sup>SM</sup> .....	89
2.3 Control Objectives for Information and related Technology - COBIT .....	90
2.3.1 COBIT IT-Governance – Die COBIT-Methodik .....	91
2.3.2 IT-Sicherheits-Überprüfung in COBIT.....	101
2.3.3 Laufende Entwicklungen von COBIT .....	107
2.4 Weitere Standards und Methodiken .....	107

2.5 Vergleich der Methodiken .....	109
2.5.1 Vergleichskriterien.....	109
2.5.2 Anwendung der Vergleichskriterien .....	111
<b>3 Methoden und Werkzeuge zur IT-Sicherheits-Überprüfung .....</b>	<b>124</b>
3.1 Penetrationstest .....	124
3.1.1 Klassifikation von Penetrationstests.....	125
3.1.2 Methodik für die Durchführung von Penetrationstests .....	129
3.2 Security Compliance Check.....	132
3.2.1 Überprüfung der Einhaltung von rechtlichen und betrieblichen Vorgaben 133	
3.2.2 Überprüfung auf Einhaltung der Sicherheitspolitiken.....	133
3.2.3 Auswertung von Protokolldateien .....	133
3.2.4 Kontrolle bestehender Verbindungen.....	134
3.2.5 Durchführung von Sicherheitskontrollen in Client-Server-Netzen	134
3.2.6 Kontrollgänge .....	135
3.3 Werkzeuge der IT-Sicherheits-Überprüfung .....	135
3.3.1 Portscanner.....	136
3.3.2 Schwachstellenscanner.....	138
3.3.3 Datenbankscanner.....	140
3.3.4 Packet Analyzer .....	140
3.3.5 Wireless Tools.....	141
3.3.6 Logfile Analyzer.....	141
3.3.7 Werkzeugsammlungen.....	142
3.3.8 Unterstützende Werkzeuge für umfassende Methodiken ....	143
<b>4 IT-Sicherheits-Überprüfungen als Dienstleistungen .....</b>	<b>145</b>
4.1 Fragebogen zur Klärung des Dienstleistungsangebots .....	145
4.2 Klassifizierung des Angebots.....	146
4.2.1 Stärken .....	151
4.2.2 Schwächen .....	151
4.3 Problematik der nichtstandardisierten Dienstleistung.....	151
<b>5 Resumee .....</b>	<b>153</b>
<b>Glossar.....</b>	<b>156</b>
<b>Anhang .....</b>	<b>164</b>
<b>Anhang A: Literatur- und Quellenverzeichnis .....</b>	<b>165</b>
<b>Anhang B: Abbildungsverzeichnis .....</b>	<b>167</b>
<b>Anhang C: Schadensgrenzen für Schutzbedarfskategorien nach IT-GSHB</b>	<b>168</b>
<b>Anhang D: Zurdnung der OCTAVE<sup>[SM]</sup> Attributes zu den OCTAVE<sup>[SM]</sup> Principles</b>	<b>170</b>

<b>Anhang E: OCTAVE[SM] Bedrohungsbäume .....</b>	<b>172</b>
<b>Anhang F: Beispiel für eine COBIT Management Guideline .....</b>	<b>175</b>
<b>Anhang G: Module für die Durchführung eines Penetrationstests ..</b>	<b>178</b>
<b>Anhang H: Fragebogen zur Klärung des Dienstleistungsangebots für IT-Sicherheits-Überprüfungen.....</b>	<b>180</b>

## Einleitung

Die Erkenntnis, dass IT-Sicherheit in unserer Gesellschaft immer wichtiger wird, setzt sich mittlerweile allgemein durch. Die Bedrohungen werden immer vielgestaltiger und häufiger.<sup>1</sup> Jedoch ist nicht jedem bewusst, dass IT-Sicherheit nicht durch einmalige Aktionen wie die Installation sicherheitstechnischer Systeme sichergestellt wird. Um die IT-Sicherheit zu gewährleisten, bedarf es des Einsatzes eines umfassenden kontinuierlichen Prozesses, welcher als IT-Sicherheitsmanagement-Prozess bezeichnet wird.

Der IT-Sicherheitsmanagement-Prozess macht eine IT-Sicherheits-Überprüfung unumgänglich. Bei den vielgestaltigen IT-Systemen, welche überall zum Einsatz kommen, stellt sich für eine Organisation jedoch die Frage nach einer idealen Methodik für die nötige IT-Sicherheits-Überprüfung. Möchte die Organisation aus irgendwelchen Gründen die IT-Sicherheits-Überprüfung nicht selbst durchführen, stellt sich darüber hinaus noch die Frage, ob und wie diese IT-Sicherheits-Überprüfungen in Österreich angeboten werden. Es ist Ziel dieser Arbeit, Antworten auf diese Fragen zu finden.

Um die Frage nach einer idealen Methodik zu Überprüfung der IT-Sicherheit zu beantworten, werden in der vorliegenden Arbeit gängige Methodiken, Methoden und Werkzeuge welche bei einer IT-Sicherheits-Überprüfung zum Einsatz kommen, untersucht und durch Einsatz von geeigneten Vergleichskriterien verglichen. Anhand der jeweiligen Vor- und Nachteile kann eine Organisation die für sie ideale Methodik auswählen.

Eine häufige Praxis in der IT-Sicherheit ist es, IT-Sicherheits-Überprüfungen von Dienstleistungsunternehmen durchführen zu lassen. Die Frage nach der Struktur des österreichischen Marktes für IT-Sicherheits-Überprüfungen wird mit Einsatz eines Fragebogens untersucht. Anhand dieser Ergebnisse wird gezeigt, welche Defizite und Perspektiven in dieser Hinsicht herrschen, und ob eine Organisation durch Inanspruchnahme einer Dienstleistung eine optimale bzw. angemessene IT-Sicherheits-Überprüfung erreichen kann.

---

<sup>1</sup> [Vgl. Symantec Corp., 2005, S. 4ff]

## **1 IT-Sicherheitsmanagement und IT-Sicherheits-Überprüfungen**

IT-Sicherheit wird in der heutigen Welt immer wichtiger. Die Abhängigkeit von Systemen zur elektronischen Datenverarbeitung und die immer weiter fortschreitende Integrierung von vernetzten Systemen in unser Leben haben es notwendig gemacht, diese Systeme vor unbefugtem Zugriff und Manipulation zu schützen. Dies geschieht durch den Einsatz eines IT-Sicherheitsmanagement-Prozesses, welcher alle Aspekte der IT-Sicherheit abdeckt und sich kontinuierlich selbst verbessert.

Von dem Begriff der IT-Sicherheit abzugrenzen ist der Begriff der Informationssicherheit, welcher die Sicherheit aller in einer Organisation befindlichen Informationen, also auch in nicht elektronischer Form, umfasst. Der in der vorliegenden Arbeit verwendete Begriff „IT-Sicherheit“ beinhaltet nicht die Sicherheit von Informationen in nicht elektronischer Form, sondern bezeichnet die Sicherheit von Systemen der Informationstechnik, welche Hardware, Software, Daten, aber auch personelle und bauliche Fragen beinhaltet, wenn sie in Zusammenhang mit der Sicherheit von IT-Systemen stehen.

### **1.1 Problemstellung: Die Suche nach der „idealen“ IT-Sicherheits-Überprüfung**

Der IT-Sicherheitsmanagement-Prozess kann sich nur selbst verbessern, wenn Defizite aufgedeckt werden. Dazu ist eine IT-Sicherheits-Überprüfung unumgänglich. Für Organisationen ergibt sich jedoch das Problem, eine ideale IT-Sicherheits-Überprüfung zu finden. Verschiedene Methodiken zur IT-Sicherheits-Überprüfung sind vorhanden, die Auswahl der besten Methodik ist jedoch nicht einfach, da die zu überprüfenden IT-Systeme höchst differenziert sind.

### **1.2 Forschungsleitende Fragestellung**

Für die betreffenden Organisationen stellt sich nun folgende Frage, welche die vorliegende Arbeit zu beantworten sucht: Gibt es eine ideale Methodik zur IT-Sicherheits-Überprüfung, und wenn ja, wie wird diese als Dienstleistung in Österreich angeboten?

### **1.3 Forschungsstrategie**

Um die Frage nach der idealen Methodik zur IT-Sicherheits-Überprüfung zu beantworten, kommt eine Inhaltsanalyse der Literatur zum Thema der Methodiken zur IT-Sicherheits-Überprüfung zum Einsatz. Die Art, wie diese Methodiken in Österreich angeboten werden,

wird durch eine Befragung von Unternehmen im Dienstleistungssektor der IT-Sicherheit beantwortet.

#### **1.4 Gründe für die Etablierung eines IT-Sicherheitsmanagement-Prozesses**

Der rasante Anstieg der Bedrohung durch freigeistig denkende Hacker und kriminelle Cracker hat zur Folge, dass IT-Infrastrukturen immer öfter Ziel von Angriffen werden. Dies wird auch verursacht durch die Verbesserung der Angriffswerkzeuge, die Angreifern zur Verfügung stehen, sowie des immer weniger notwendigen Sachverständnisses seitens der Angreifer, diese Werkzeuge zu benutzen. Auch die Fülle der Sicherheitsschwächen in IT-Netzwerken bietet den Angreifern genügend Möglichkeiten, zum Erfolg zu kommen.<sup>2</sup>

#### **Datenschutzgesetz**

Unternehmen sind gesetzlich durch das österreichische DSG (=Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idF. BGBl. I Nr. 136/2001) dazu verpflichtet, Personen-daten vor unerlaubtem Zugriff und Zerstörung zu schützen:

„Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist [...] sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.“ (DSG 2000 , BGBl. I Nr. 165/1999 Abschnitt 3, §14 Abs. 1)

Das DSG liegt unter <http://www.dsk.gv.at/dsg2000d.htm> auf.

#### **Bedrohungen**

Seit dem Beginn der Aufzeichnungen von vorgefallenen *Incidents* (= sicherheitsrelevante Vorfälle) durch das *CERT®/CC* (=CERT® Coordination Center) der Carnegie Mellon University im Jahre 1988 stieg die Anzahl der aufgezeichneten Incidents pro Jahr stetig an. Im Laufe des Jahres 2004 wurde sogar auf eine Statistik der Incidents verzichtet, da Angriffe durch automatisierte Angriffswerkzeuge mittlerweile so weit verbreitet sind, dass die Anzahl der Incidents kein aussagekräftiger Indikator für die tatsächliche Bedrohung mehr ist.<sup>3</sup> Eine Bedrohung ist somit in jedem Fall gegeben und kann nicht ignoriert werden. Dieses Bewusstsein

---

<sup>2</sup> [Vgl. Hahnbauer 2003, S. 1 ff]

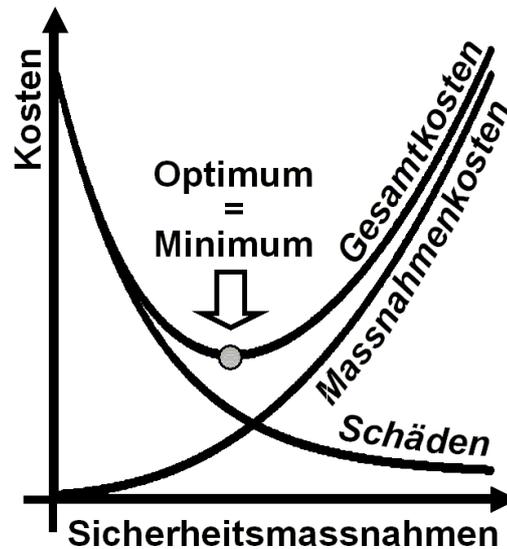
hat die Installation von sicherheitstechnischen Systemen vorangetrieben. Das Wissen um deren Notwendigkeit hat sich von den IT-Abteilungen der Unternehmen und Organisationen ins mittlere bis höhere Management verbreitet. Dennoch ist das Ergebnis dieser Entwicklung keineswegs eine Lösung des Problems, da einige Missverständnisse, wie die Annahme, Sicherheit wäre technisch lösbar, einer hohen IT-Sicherheit im Wege stehen.

### **Kosten**

IT-Sicherheit ist nicht billig. Diese leidvolle Erfahrung mussten vor allem die zuständigen Mitarbeiter eines Unternehmens in der nahen Vergangenheit machen, wenn sie Ausgaben im Bereich der IT-Sicherheit gegenüber dem Management rechtfertigen mussten. Dies galt vor allem, bevor die Notwendigkeit der Etablierung einer effektiven IT-Sicherheit auch den höheren Ebenen des Managements bekannt war. Durch die erfolgte Bewusstseinsbildung wurde das Problem verringert, jedoch nicht beseitigt. Dabei besteht kein Grund, bei der IT-Sicherheit zu sparen. Im Gegenteil: Ein hoher Standard der IT-Sicherheit ist eine Investition, welche den Wert des Unternehmens steigert. Die Verluste, welche ein Unternehmen durch Angriffe erleiden kann, werden durch die zunehmende Integrierung der IT-Systeme in den Geschäftsablauf sowie der steigenden Anzahl der Incidents immer gravierender. Sie betreffen Produktionsausfälle, Imageverluste oder Verlust von Geschäftsgeheimnissen (Industriespionage). Bei steigenden Kosten durch Schäden, welche durch eine bessere IT-Sicherheit verhindert werden könnten, wird die Investition in die IT-Sicherheit immer dringlicher. Die Kosten für das Unternehmen belaufen sich auf die Summe aus Investitionen und Kosten durch Schadensfälle. Das Ziel ist es, ein Minimum dieser Kosten zu finden (s. Abb. 1-1)

---

<sup>3</sup> [Vgl. CERT®/CC, 19.10.2004, 1, CERT®/CC Statistics 1988-2004, [http://www.cert.org/stats/cert\\_stats.html#incidents](http://www.cert.org/stats/cert_stats.html#incidents) ]



**Abbildung 1-1: Kostenoptimierung für die IT-Sicherheit**

Quelle: VBS, 5.3.2004,

<http://www.vbs-ddps.ch/internet/groupgst/de/home/integrale0/objektschutz0.html>

Wurde durch eine Betrachtung dieser Sachlage eine erhöhte Investition in die IT-Sicherheit erreicht, wird die Frage nach den richtigen Investitionen laut. Auch hier wurde und wird vieles immer noch falsch gemacht. Viele Unternehmen investieren hauptsächlich in Sicherheitstechnologien. Dies geschieht aufgrund der Fehlannahme, dass verbreitete Sicherheitstechnologien auch ohne laufende Wartungen und Investitionen Sicherheit bieten. Dies kann sich als folgenschwerer Irrtum herausstellen.

### **Sicherheit von der Stange**

Viele Unternehmen begingen in den letzten Jahren den Fehler, das Budget für IT-Sicherheit in singuläre Maßnahmen und Technologien zu investieren. Einmalige Investitionen bringen aber keinen langfristigen Vorteil, wenn sie nicht durch regelmäßige Wartung und Revision den ständig wechselnden Gegebenheiten angepasst werden. Der Einsatz von Firewalls ist dafür ein bekanntes Beispiel. Oftmals erwarben Unternehmen eine Firewall und hiermit ein subjektives Gefühl von Sicherheit, ohne jedoch zu realisieren, dass Sicherheit nicht durch Installation eines einzelnen Systems sichergestellt werden kann. Dies trifft vor allem zu, wenn die Installation nicht mit dem nötigen Fachwissen durchgeführt wurde. Eine Firewall kann so

nur einen Bruchteil ihres Nutzens tatsächlich erbringen. Auch in diesem Bereich ist eine Bewusstseinsbildung im Gange.

In den letzten Jahren wurde zunehmend deutlich, dass eine effektive IT-Sicherheit nicht allein durch einzelne Maßnahmen wie beispielsweise Virenschutz oder Installationen von Firewalls und *IDS* (= Intrusion Detection System) sichergestellt werden kann. Vielmehr ist es notwendig, ein umfassendes IT-Sicherheitsmanagement zu etablieren, welches die IT-Security in den Managementprozess integriert.<sup>4</sup>

### 1.5 Der IT-Sicherheitsmanagementprozess

Das Ö-IT-SIHB (=Österreichische IT-Sicherheitshandbuch) schreibt über das IT-Sicherheitsmanagement:

*„IT-Sicherheitsmanagement ist ein kontinuierlicher Prozess, der die Sicherheit und Zuverlässigkeit von Systemen der Informationstechnik (IT-Systemen) innerhalb einer Organisation gewährleisten soll.“<sup>5</sup>*

Das Ö-IT-SIHB liefert einen auf das GSHB (=Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik) ausgerichteten Leitfaden zur Etablierung eines IT-Sicherheitsmanagement-Prozesses. Integraler Bestandteil eines IT-Sicherheitsmanagement-Prozesses ist die Überprüfung der IT-Sicherheit in verschiedenen Ausprägungen, welche Thema der vorliegenden Arbeit sind. Doch zunächst ist ein Blick auf die Aufgaben des IT-Sicherheitsmanagements von Interesse:<sup>6</sup>

- Festlegung der IT-Sicherheitsziele, -strategien und –politiken der Organisation,
- Festlegung der IT-Sicherheitsanforderungen,
- Ermittlung und Analyse von Bedrohungen und Risiken,
- Festlegung geeigneter Sicherheitsmaßnahmen,
- Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Maßnahmen,
- Förderung des Sicherheitsbewusstseins innerhalb der Organisation sowie
- Entdecken von und Reaktion auf sicherheitsrelevante Ereignisse

---

<sup>4</sup> [Vgl. Ö-IT-SIHB Teil 1, S. 7]

<sup>5</sup> [Ö-IT-SIHB Teil 1, S. 7]

<sup>6</sup> [Vgl. Ö-IT-SIHB Teil 1, S. 7]

Die Erfüllung der Aufgaben des IT-Sicherheitsmanagements ist Ziel des IT-Sicherheitsmanagement-Prozesses. Er besteht aus fünf Teilschritten, welche im Grunde auf sich selbst zurückführen, stellt also einen kontinuierlichen Prozess dar. Die fünf Schritte sind im Einzelnen:<sup>7</sup>

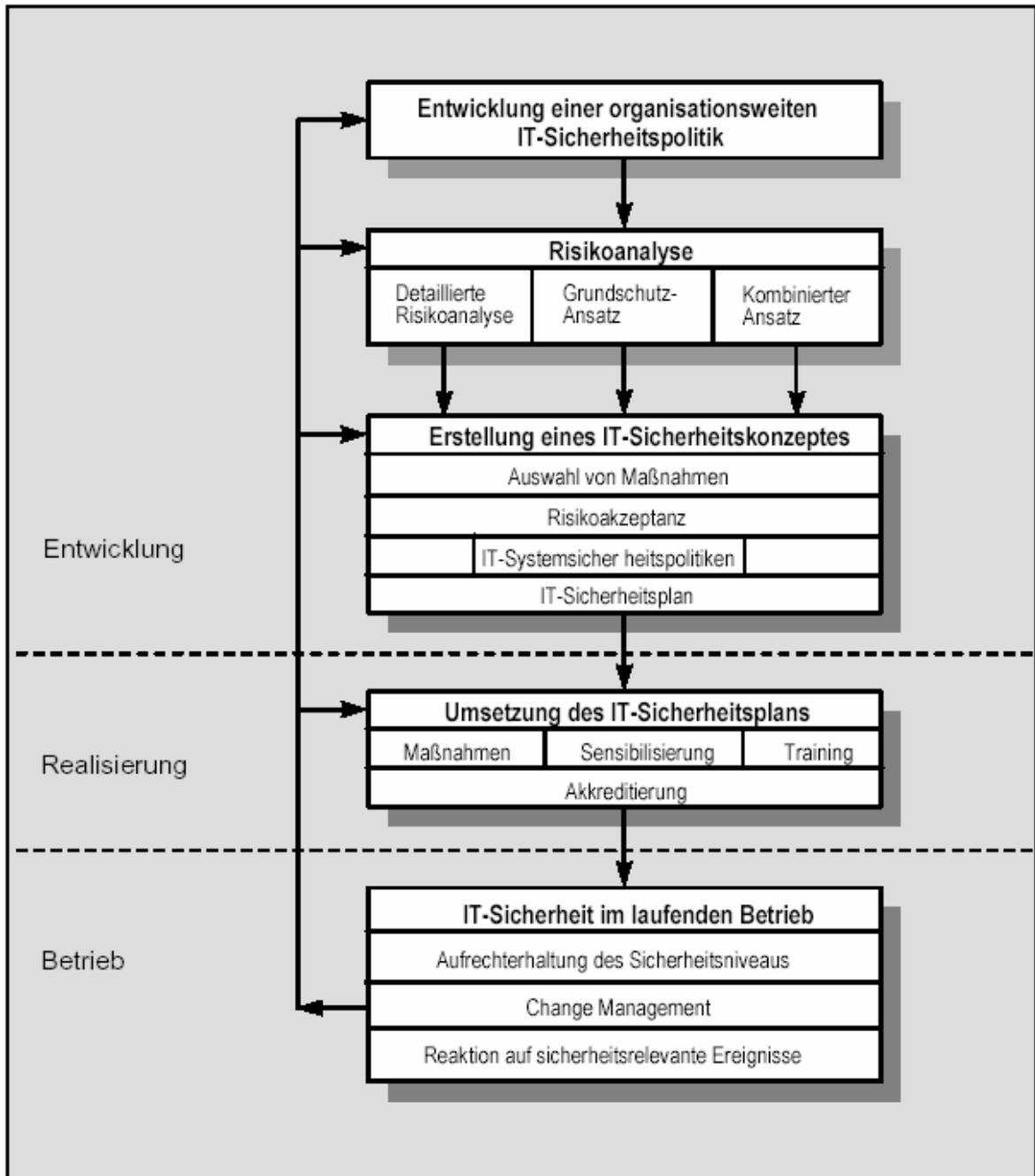
1. Entwicklung einer organisationsweiten IT-Sicherheitspolitik
2. Durchführung einer Risikoanalyse
3. Erstellung eines IT-Sicherheitskonzeptes
4. Erstellung eines IT-Sicherheitsplanes
5. Gewährleistung der IT-Sicherheit im laufenden Betrieb

Der hier vorgestellte IT-Sicherheitsmanagement-Prozess aus dem Ö-IT-SIHB basiert auf internationalen Standards und Leitlinien, insbesondere den „Guidelines on the Management of IT-Security (GMITS)“ ([ISO/IEC 13335]).

Abbildung 1-2 verdeutlicht die Aktivitäten im Rahmen des IT-Sicherheitsmanagements.

---

<sup>7</sup> [Vgl. Ö-IT-SIHB Teil 1, S. 10]



**Abbildung 1-2: Aktivitäten im Rahmen des IT-Sicherheitsmanagements**

Quelle: Ö-IT-SIHB, Teil 1, S. 11

Bevor die Rolle der IT-Sicherheits-Überprüfungen im IT-Sicherheitsmanagement näher beleuchtet wird, folgt eine Betrachtung der Teilschritte des IT-Sicherheitsmanagement-Prozesses.

### 1.5.1 Entwicklung einer organisationsweiten IT-Sicherheitspolitik

Über die IT-Sicherheitspolitik schreibt das Ö-IT-SIHB:

*„Als organisationsweite IT-Sicherheitspolitik (Corporate IT Security Policy) bezeichnet man die Leitlinien und Vorgaben innerhalb einer Organisation, die unter Berücksichtigung gegebener Randbedingungen grundlegende Ziele, Strategien, Verantwortlichkeiten und Methoden für die Gewährleistung der IT-Sicherheit festlegen.“<sup>8</sup>*

Die IT-Sicherheitspolitik ist ein langfristig orientiertes Grundlagendokument, welches für den gesamten Einsatzbereich der IT im Unternehmen Gültigkeit hat. Es handelt sich um ein über die Zeit gesehen statisches Dokument, welches nicht auf technologische Details oder spezifische Sicherheitsmaßnahmen eingeht.<sup>9</sup> Die organisationsweite IT-Sicherheitspolitik wird von den nachfolgenden IT-Systemsicherheitspolitiken (z.B. PC-Sicherheitspolitik oder Netzwerksicherheitspolitik) spezifiziert.<sup>10</sup> Der genaue Ablauf der Erstellung einer IT-Sicherheitspolitik geht über den Rahmen dieser Arbeit hinaus. Da jedoch die IT-Sicherheitspolitik als Grundlagendokument von großer Wichtigkeit ist, und ihr Vorhandensein bzw. ihre Vollständigkeit und Einhaltung bei IT-Sicherheits-Überprüfungen eine wichtige Rolle spielt, ist ein kurzer Überblick durchaus angebracht.

Folgende Inhalte finden sich in einer IT-Sicherheitspolitik:<sup>11</sup>

- IT-Sicherheitsziele und Strategien
- Organisation und Verantwortlichkeiten für IT-Sicherheit
- Risikoanalysestrategien, akzeptables Restrisiko und Akzeptanz von außergewöhnlichen Restrisiken
- Klassifizierung von Daten
- Klassifizierung von IT-Anwendungen und IT-Systemen, Grundzüge der Business Continuity Planung
- Nachfolgeaktivitäten zur Überprüfung und Aufrechterhaltung der IT-Sicherheit

Die in der IT-Sicherheitspolitik niedergelegten Ziele sind beispielsweise die Einhaltung gesetzlicher Vorgaben, die Gewährleistung des Vertrauens der Kunden in das Unternehmen, die

---

<sup>8</sup> [Ö-IT-SIHB, Teil 1, S. 11]

<sup>9</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 11]

<sup>10</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 14]

<sup>11</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 15-27]

Sicherung der investierten Werte oder die Reduzierung der im Schadensfall verursachten Kosten. Meist gehen die veranschlagten Ziele über diese Beispiele hinaus.

Die Ziele der IT-Sicherheitspolitik führen zu einem gewünschten IT-Sicherheits-Niveau, welches erreicht werden soll, um die genannten Ziele zu erfüllen. Der nächste Schritt ist die Auswahl der IT-Sicherheits-Strategien, mit denen das gewünschte Niveau der IT-Sicherheit erreicht werden soll. Beispiele für strategische Entscheidungen dieser Art sind die Einführung eines organisationsweiten *Incident Handling Plans* und die klare Zuordnung von Verantwortlichkeiten für die IT-Sicherheit innerhalb der Organisation.

Ist die IT-Sicherheitspolitik erstellt, dienen ihre Vorgaben (vor allem die Feststellung, welche Teile des IT-Systems besonders wichtig zur Erreichung der strategischen Ziele sind) als Input für den zweiten Schritt des IT-Sicherheitsmanagement-Prozesses.

### 1.5.2 Risikoanalyse

*„Eine wesentliche Voraussetzung für erfolgreiches IT-Sicherheitsmanagement ist die Einschätzung der bestehenden Sicherheitsrisiken. In einer Risikoanalyse wird versucht, diese Risiken zu erkennen und zu bewerten und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.“<sup>12</sup>*

Zur Durchführung einer Risikoanalyse gibt es verschiedene Strategien, das Ö-IT-SIHB behandelt die drei wichtigsten davon.<sup>13</sup>

#### Detaillierte Risikoanalyse

Bei dieser Methode wird für jedes IT-System eine detaillierte Risikoanalyse durchgeführt, was zu effektiven Sicherheitsmaßnahmen, jedoch auch zu einer langen Dauer und hohen Kosten führt. Die detaillierte Risikoanalyse, welche eine Dauer von Wochen oder sogar Monaten haben kann, besteht im Wesentlichen aus acht Schritten, welche hier in aller Kürze vorgestellt werden, wobei das Ö-IT-SIHB zitiert wird.<sup>14</sup>

---

<sup>12</sup> [Ö-IT-SIHB, Teil 1, S. 29]

<sup>13</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 29]

<sup>14</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 30f]

### **1. Identifikation des bedrohten Systems**

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

### **2. Identifikation der bedrohten Objekte**

Ziel dieses Schrittes ist die Erfassung aller bedrohten Objekte, die innerhalb des im vorangegangenen Schritt festgesetzten Analysebereiches liegen.

### **3. Wertanalyse**

In diesem Schritt wird der Wert der bedrohten Objekte ermittelt.

Die Wertanalyse umfasst im Einzelnen:

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

### **4. Bedrohungsanalyse**

Die Objekte sind vielfachen Bedrohungen ausgesetzt, die sowohl aus Nachlässigkeit und Versehen als auch aus Absicht resultieren können.

Die Bedrohungsanalyse umfasst:

- Die Identifikation möglicher Bedrohungen (Katastrophen, Fehlbedienungen, bewusste Angriffe) und möglicher Angreifer (Mitarbeiter, Leasingpersonal, Außenstehende,...)
- Die Ermittlung der Eintrittswahrscheinlichkeiten

### **5. Schwachstellenanalyse**

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Es ist daher erforderlich, mögliche Schwachstellen des Systems zu identifizieren und ihre Bedeutung zu klassifizieren.

Zu untersuchen sind dabei insbesondere die Bereiche Organisation, Hard- und Software, Personal sowie Infrastruktur.

### **6. Identifikation bestehender Sicherheitsmaßnahmen**

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

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

### **7. Risikobewertung**

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

### **8. Auswertung und Aufbereitung des Ergebnisses**

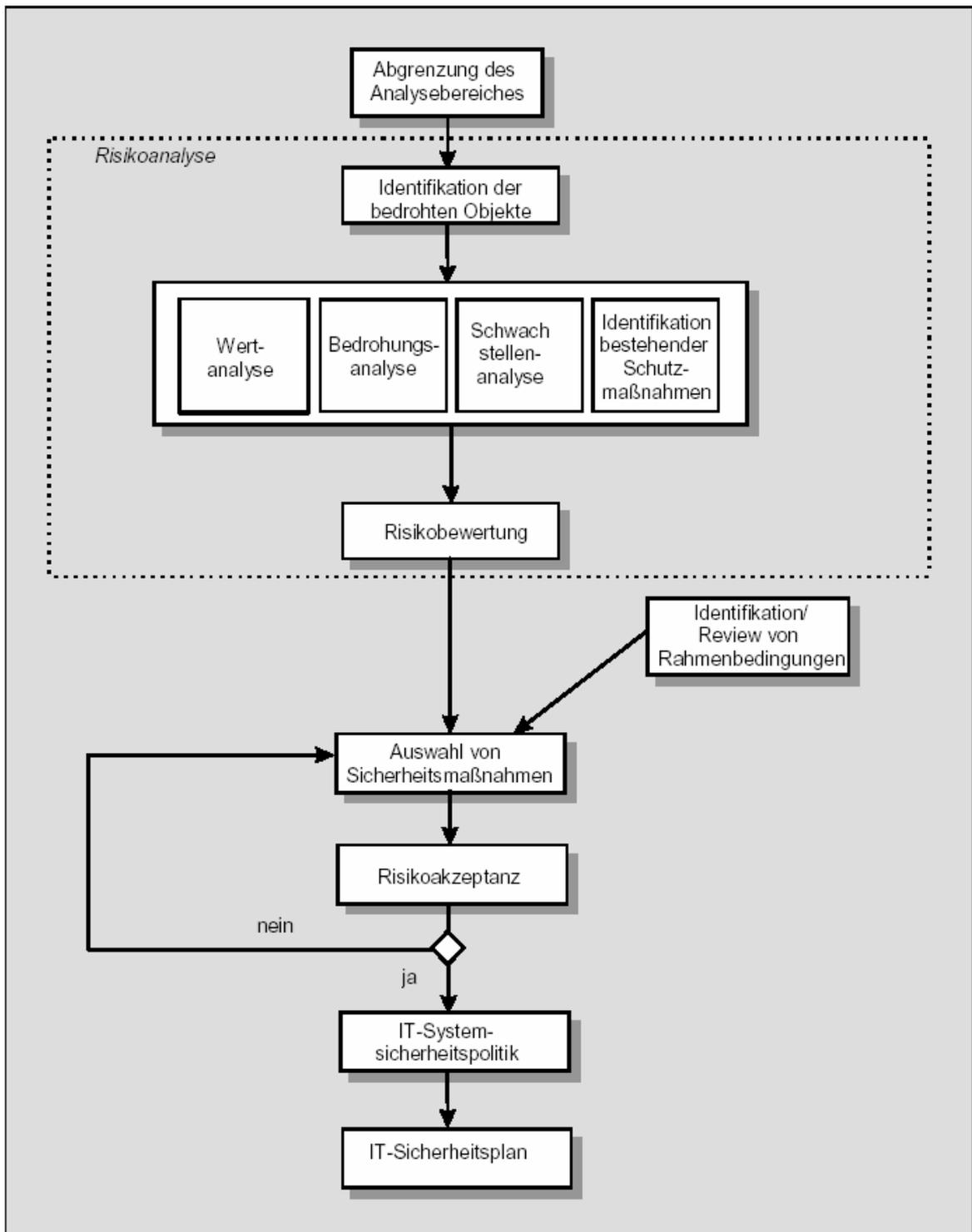
Eine Auswertung und Aufbereitung des Ergebnisses schließt die Risikoanalyse ab.

Der Ablauf der detaillierten Risikoanalyse und ihre Einbettung in den IT-Sicherheitsmanagement-Prozess werden in Abb. 1-3 dargestellt.

Eine bei der detaillierten Risikoanalyse benutzte Methode zur IT-Sicherheits-Überprüfung ist die *Schwachstellenanalyse*. Eine *Schwachstelle* (=vulnerability) ist eine Sicherheitsschwäche in einem oder mehreren Objekten, die durch eine Bedrohung ausgenutzt werden kann. Beispiele hierfür sind schwache Passwortmechanismen ebenso wie mindersichere Türschlösser. Schwachstellen alleine verursachen keinen Schaden. Sobald allerdings eine korrespondierende Bedrohung existiert, sollte umgehend reagiert werden. Eine Schwachstellenanalyse ist eine Überprüfung von Sicherheitsschwächen, welche durch Bedrohungen ausgenutzt werden können. Das Ergebnis der Schwachstellenanalyse ist eine Liste der Schwachstellen und eine Einschätzung, wie leicht diese ausgenutzt werden können.<sup>15</sup>

---

<sup>15</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 37f]



**Abbildung 1-3: Risikomanagement mit detaillierter Risikoanalyse**

Quelle: Ö-IT-SIHB, Teil 1, S. 32

## **Grundschutzansatz**

Der zweite Ansatz zur Risikoanalyse ist der Grundschutzansatz. Die Idee hinter dem Grundschutzansatz ist, den Aufwand für die Erstellung eines IT-Sicherheitskonzeptes angemessen zu begrenzen. Dies geschieht durch die Annahme einer pauschalisierten Gefährdungslage und Verzicht auf eine detaillierte Risikoanalyse. Für die verschiedenen IT-Systeme wird von einem Katalog von Gefährdungen ausgegangen, welchen mit einem Katalog von Schutzmaßnahmen (Grundschutzmaßnahmen) begegnet wird. Für jedes IT-System (Modul) schreibt dieser Grundschutzkatalog die zu treffenden Maßnahmen vor. Dies hat den Vorteil, den Aufwand für die Risikoanalyse in Form von Zeit und Geld stark zu reduzieren. Darüber hinaus führt der Ansatz schnell zu einem relativ hohen Niveau an Sicherheit gegenüber den häufigsten Bedrohungen.<sup>16</sup>

Nachteile des Grundschutzansatzes sind die mögliche Unangemessenheit des Grundschutzes für das spezielle System, was zu wenig Schutz bzw. Verschwendung von Mitteln bei zu hohem Schutz bedeutet.<sup>17</sup>

An dieser Stelle muss erwähnt werden, dass das deutsche Bundesamt für Sicherheit in der Informationstechnik ein umfangreiches Handbuch zur Grundschutzmethode entwickelt hat, welches im zweiten Kapitel der vorliegenden Arbeit im Kontext der Methodiken zur IT-Sicherheits-Überprüfung betrachtet wird.

## **Kombinierter Ansatz**

Die dritte Methode der Risikoanalyse bietet einen kombinierten Ansatz. Sie beginnt mit einer Schutzbedarfsfeststellung (High Level Risk Analysis). Für nicht-kritische IT-Systeme (Schutzbedarf niedrig bis mittel) kommt der Grundschutz zum Einsatz, bei besonders schutzbedürftigen Systemen (Schutzbedarf hoch bis sehr hoch) wird eine detaillierte Risikoanalyse durchgeführt. Diese Methode verbindet die Vorteile der anderen beiden. Sie verhilft zu einem hohen Niveau an IT-Sicherheit an jenen Stellen, wo sie notwendig ist, und erlaubt eine schnelle und effektive Implementierung der Sicherheit an weniger kritischen Systemen. Im Regelfall ist dieser Ansatz den anderen vorzuziehen.<sup>18</sup> Abb. 1-4 verdeutlicht den Ablauf.

---

<sup>16</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 40]

<sup>17</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 40]

<sup>18</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 44]



**Abbildung 1-4: Kombinerter Ansatz**

Quelle: Ö-IT-SIHB, Teil 1, S. 44

Der kombinierte Ansatz verfügt über folgende Stärken und Schwächen:<sup>19</sup>

- Rasche Erreichung eines relativ guten Sicherheitsniveaus für alle IT-Systeme
- Die Schutzbedarfsfestellung kann als Basis für eine Prioritätenreihung der nachfolgenden Aktivitäten dienen
- Konzentration des Aufwandes auf jene Teile des IT-Systems, welche den Aufwand benötigen
- Hohe Akzeptanz durch rasch sichtbare Erfolge bei geringem Initialaufwand
- Grundsätzlich das Risiko, einem IT-System mit hohem Schutzbedarf fälschlicherweise einen niedrigeren Schutzbedarf zuzuordnen. Eine derartige Fehlentscheidung lässt das betreffende IT-System allerdings nicht ungeschützt, da zumindest die Grundschutzmaßnahmen getroffen werden.

Der kombinierte Ansatz ist dadurch die vom Ö-IT-SIHB empfohlene Vorgangsweise zur Risikoanalyse.

### **Akzeptables Restrisiko**

Sicherheitsmaßnahmen können in der Regel nicht alle festgestellten Risiken mindern bzw. ausschalten. Für gewöhnlich bleibt ein Restrisiko erhalten, welches bewusst akzeptiert werden muss, da seine Abdeckung wirtschaftlich nicht vertretbar wäre. Dieses Restrisiko muss in der IT-Sicherheitspolitik möglichst exakt quantifiziert werden.<sup>20</sup>

<sup>19</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 44f]

<sup>20</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 48f]

## **Akzeptanz von außergewöhnlichen Restrisiken**

Falls nach Durchführung aller Sicherheitsmaßnahmen ein Restrisiko bestehen bleibt, welches höher ist als das akzeptable, sollten zusätzliche Maßnahmen getroffen werden. Ist dies technisch oder wirtschaftlich nicht möglich, so kann das Management in begründeten Fällen dieses Restrisiko akzeptieren. Die Verantwortlichkeiten dafür müssen in der IT-Sicherheitspolitik schriftlich festgehalten werden.<sup>21</sup>

Nach der Durchführung der Risikoanalyse folgt im IT-Sicherheitsmanagement-Prozess die Erstellung eines IT-Sicherheitskonzeptes.

### **1.5.3 Erstellung von IT-Sicherheitskonzepten**

Das Ö-IT-SIHB schreibt über IT-Sicherheitskonzepte:

*„Ausgehend von den in der Risikoanalyse ermittelten Sicherheitsanforderungen wird ein IT-Sicherheitskonzept erstellt. Dies erfolgt durch die Auswahl geeigneter Maßnahmen, die die Risiken auf ein akzeptables Maß reduzieren und unter dem Gesichtspunkt von Kosten und Nutzen eine optimale Lösung darstellen.“<sup>22</sup>*

Inhalt eines IT-Sicherheitskonzeptes ist:<sup>23</sup>

- Die Beschreibung des Ausgangszustandes und Ergebnisse der Risikoanalyse
- Die Festlegung der durchzuführenden Maßnahmen.
- Die Begründung der Auswahl hinsichtlich Kosten/Nutzen-Aspekten und Zusammenspiel der einzelnen Maßnahmen
- Abschätzung des Restrisikos und eine verbindliche Aussage über akzeptables Restrisiko
- Die Festlegung der Verantwortlichkeiten für die Auswahl und Umsetzung der Maßnahmen sowie für die regelmäßige Überprüfung des Konzeptes
- Die Planung für die Umsetzung inklusive Prioritäten und Ressourcenplanung.

Das IT-Sicherheitskonzept ist eine Auswahl an Maßnahmen, welche die Ziele der IT-Sicherheitspolitik in Anpassung an das gegebene Risiko umsetzen soll. Seine Erstellung erfolgt in vier Schritten:<sup>24</sup>

---

<sup>21</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 49]

<sup>22</sup> [Ö-IT-SIHB, Teil 1, S. 50]

<sup>23</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 50]

<sup>24</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 50]

1. Auswahl von Maßnahmen
2. Risikoakzeptanz
3. Erstellung von IT-Systemsicherheitspolitiken
4. Erstellung eines IT-Sicherheitsplanes

Sicherheitsmaßnahmen sind Verfahrensweisen, welche die Sicherheit eines Systems erhöhen, indem sie:

- Risiken vermeiden,
- Bedrohungen oder Schwachstellen verkleinern,
- Unerwünschte Ereignisse entdecken,
- die Auswirkung eines unerwünschten Ereignisses eingrenzen,
- Risiken überwälzen oder
- es möglich machen, einen früheren Zustand wiederherzustellen.

Sicherheitsmaßnahmen können verschiedenartig klassifiziert werden. Mögliche Klassifizierungen sind jene nach der Art der Maßnahmen (technischer, organisatorischer, baulicher oder personeller Art), dem Bereich der Anwendung (organisationsweit oder systemspezifisch) oder nach den Gefährdungen bzw. Sicherheitsanforderungen. Letztere sind Maßnahmen, welche die Vertraulichkeit (confidentiality), Integrität (integrity), Verfügbarkeit (availability), Zurechenbarkeit (accountability), Authentizität (authenticity) oder Zuverlässigkeit (reliability) sicherstellen sollen. Verluste dieser Qualitäten sind die Grundbedrohungen gegen jedes IT-System.<sup>25</sup>

---

<sup>25</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 51f]

## **Auswahl von Maßnahmen**

Sicherheitsmaßnahmen werden ausgehend von der Risikoanalyse ausgewählt, sind also demnach spezielle Maßnahmen, welche auf das detaillierte Risiko der IT-Systeme ausgerichtet sind, oder auch Grundschutzmaßnahmen. Bei der Auswahl der Sicherheitsmaßnahmen ist immer zu beachten, welche Sicherheitsmaßnahmen bereits bestehen.<sup>26</sup>

## **Risikoakzeptanz**

Wie bereits ausgeführt, ist das Risiko nicht vollständig auszuschalten. Eine Grundlage für die Einteilung der Restrisiken in die Klassen „akzeptabel“ und „nicht akzeptabel“ sollte in der organisationsweiten IT-Sicherheitspolitik festgelegt sein. Bei der Erstellung des IT-Sicherheitskonzeptes werden die Restrisiken (nach Auswahl der Sicherheitsmaßnahmen) auf Grundlage der zuvor stattgefundenen Risikoanalyse möglichst exakt quantifiziert. „Akzeptable“ Restrisiken werden akzeptiert, „nicht akzeptable“ bedürfen einer weiteren Analyse.<sup>27</sup>

## **Erstellung von IT-Systemsicherheitspolitiken**

IT-Systemsicherheitspolitiken sind genau wie die organisationsweiten IT-Sicherheitspolitiken Basisdokumente. Sie sind der organisationsweiten IT-Sicherheitspolitik untergeordnet, kommen also nur für spezielle IT-Systeme zum Einsatz, dürfen allerdings nicht zur organisationsweiten IT-Sicherheitspolitik im Widerspruch stehen. Abbildung 1-5 verdeutlicht die Einordnung der IT-Systemsicherheitspolitiken in die Organisationspolitik.<sup>28</sup>

Inhalt der IT-Systemsicherheitspolitik sind unter anderem die für das betreffende System bereits realisierten bzw. noch zu realisierenden Sicherheitsmaßnahmen, Schwachstellen des Systems, Sicherheitsrisiken und die Festlegung der IT-Sicherheitsziele des betreffenden IT-Systems.<sup>29</sup>

IT-Systemsicherheitspolitiken sind regelmäßig auf Aktualität zu prüfen und dementsprechend anzupassen. Von besonderer Bedeutung ist die Aktualität der noch zu realisierenden Sicherheitsmaßnahmen.<sup>30</sup>

---

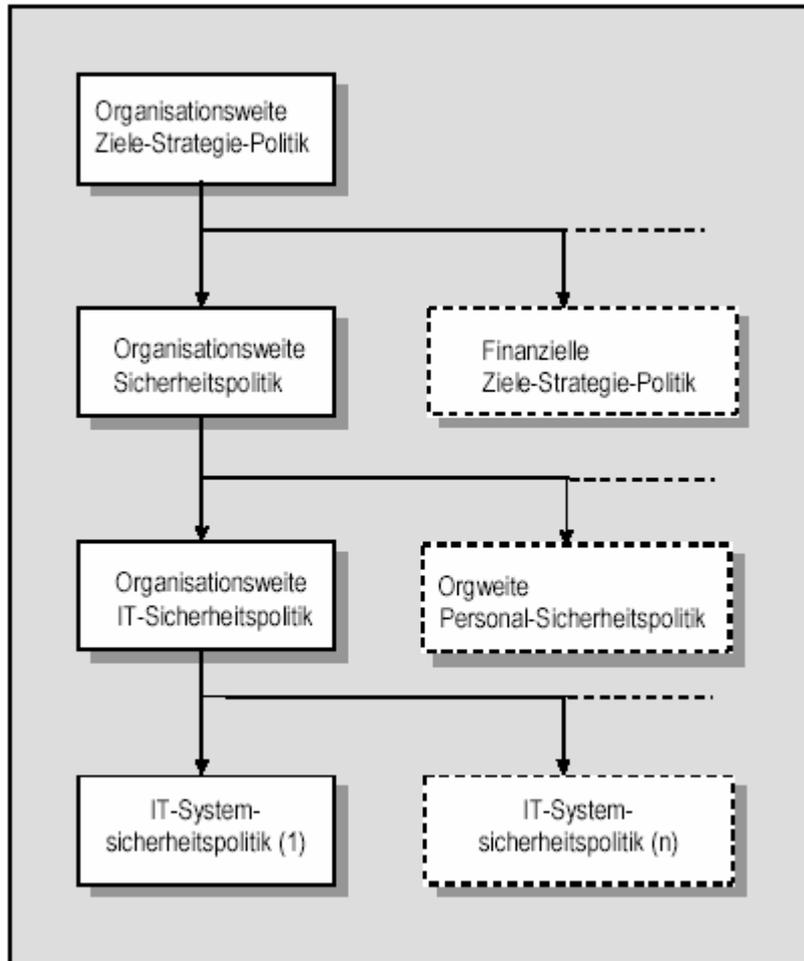
<sup>26</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 52]

<sup>27</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 55f]

<sup>28</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 56]

<sup>29</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 57]

<sup>30</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 57f]



**Abbildung 1-5: Einbettung der IT-Systemsicherheitspolitik in die Regelungen der Organisation**

Quelle: Ö-IT-SIHB, Teil 1, S. 57

### Erstellung eines IT-Sicherheitsplanes

Nachdem die einzusetzenden Sicherheitsmaßnahmen beschlossen und die Systemsicherheitspolitiken erstellt wurden, wird ein IT-Sicherheitsplan erstellt. Dieser beschreibt, wie die gewählten Sicherheitsmaßnahmen umgesetzt werden. Dies beinhaltet eine Prioritäten- und Ressourcenplanung sowie einen Zeitplan für die Umsetzung. Weiters sollte der IT-Sicherheitsplan auch Kontrollmechanismen definieren, die den Fortschritt der Implementierung überwachen.<sup>31</sup>

<sup>31</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 58]

Der IT-Sicherheitsplan muss ebenfalls laufend umgeschrieben werden, um beispielsweise auf neue Bedrohungen oder geänderte Organisationsziele angepasst zu werden, oder nach einer Untersuchung des IT-Sicherheitsplanes nach Ablauf eines bestimmten Zeitraumes.<sup>32</sup>

### 1.5.4 Umsetzung des IT-Sicherheitsplanes

Sobald der IT-Sicherheitsplan erstellt wurde, erfolgt seine Umsetzung in vier Schritten:<sup>33</sup>

1. Implementierung der Maßnahmen
2. Sensibilisierung (*Security Awareness*)
3. Schulung
4. Akkreditierung

#### Implementierung der Maßnahmen

Sobald der IT-Sicherheitsplan erstellt wurde, ist es an der Zeit, die einzelnen Maßnahmen anzuwenden, auf ihre Konformität zur IT-Sicherheitspolitik zu prüfen (= *Security Compliance Checking*) und auf ihre Korrektheit und Vollständigkeit zu testen.<sup>34</sup>

#### Sensibilisierung (Security Awareness)

IT-Sicherheit kann ohne weiteres durch unsachgemäßen Umgang mit dem IT-System nutzlos werden. Die Ausbildung eines Sicherheitsbewusstseins bei den Benutzern ist deshalb sehr wichtig. Diesen Vorgang nennt man Sensibilisierung. IT-Sicherheit geht alle Mitarbeiter der Organisation etwas an und sollte mithilfe eines Sensibilisierungsprogrammes in den täglichen Arbeitsprozess integriert werden.<sup>35</sup>

#### Schulung

Über die Sensibilisierung hinausgehende Schulungen sind dann notwendig, wenn die Sicherheitsmaßnahmen drastische Veränderungen, z.B. im Arbeitsablauf, bedingen. Darüber hinaus müssen Mitarbeiter, die besondere Tätigkeiten im IT-Sicherheitsmanagement innehaben oder durch die Art ihrer Tätigkeit in engem Kontakt dazu kommen, speziell für ihre Aufgaben

---

<sup>32</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 59]

<sup>33</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 60]

<sup>34</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 60ff]

<sup>35</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 62f]

geschult werden. Typische Vertreter dieser Gruppe sind Systemadministratoren, IT-Sicherheitsbeauftragte und Projektleiter im IT-Bereich.<sup>36</sup>

### **Akkreditierung**

Die Akkreditierung ist der letzte Schritt bei der Umsetzung des IT-Sicherheitsplans. Laut Ö-IT-SIHB versteht man unter Akkreditierung eines IT-Systems

*„[...] die Sicherstellung, dass dieses [IT-System] den Anforderungen der IT-Systemsicherheitspolitik und des IT-Sicherheitsplanes genügt.“<sup>37</sup>*

Dabei ist besonders auf die Sicherstellung zu achten, dass die Sicherheit des IT-Systems

- in einer bestimmten Betriebsumgebung,
- unter bestimmten Einsatzbedingungen und
- für eine bestimmte Zeitspanne

gewährleistet ist. Erst nach dieser Bestätigung kann das betreffende IT-System in Echtbetrieb gehen. Für die Akkreditierung gibt es verschiedene Techniken:<sup>38</sup>

- Security Compliance Checking
- Tests
- Evaluation und Zertifizierung des Systems

Veränderungen in der Betriebsumgebung oder den eingesetzten Sicherheitsmaßnahmen können eine neuerliche Akkreditierung notwendig machen. Die Kriterien dafür sollten in der IT-Sicherheitspolitik festgelegt sein.<sup>39</sup>

#### **1.5.5 IT-Sicherheit im laufenden Betrieb**

Als letzter Teil des IT-Sicherheitsmanagement-Prozesses steht die Aufgabe, die IT-Sicherheit im laufenden Betrieb sicherzustellen. Ständige Überprüfung der Wirksamkeit, Aktualität und Akzeptanz der getroffenen Maßnahmen ist ungemein wichtig. Ebenso müssen Reaktionen auf Incidents oder Veränderungen der Technologien in das IT-Sicherheitskonzept eingearbeitet werden. Dies wird durch eine Rückkopplung der Erkenntnisse aus dem laufenden Betrieb erreicht. Das Ziel der Aktivitäten im laufenden Betrieb ist es, das erreichte IT-

---

<sup>36</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 63f]

<sup>37</sup> [Ö-IT-SIHB, Teil 1, S. 64]

<sup>38</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 64]

<sup>39</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 64]

Sicherheitsniveau zu halten oder zu steigern. Verschlechterungen des IT-Sicherheitsniveaus sollen erkannt werden und entsprechende Gegenmaßnahmen einleiten. Um all diese Ziele zu erreichen, finden im laufenden Betrieb folgende Aktivitäten statt:<sup>40</sup>

- Aufrechterhaltung des erreichten IT-Sicherheitsniveaus
- *Change Management* (= Aktivitäten bei Änderungen des IT-Systems)
- *Incident Handling* (= Reaktion auf sicherheitsrelevante Ereignisse)

### **Aufrechterhaltung des erreichten IT-Sicherheitsniveaus**

Um nach der Umsetzung des IT-Sicherheitsplanes das erreichte IT-Sicherheitsniveau aufrechtzuerhalten, müssen folgende Tätigkeiten unternommen werden:<sup>41</sup>

- Wartung und administrativer Support der Sicherheitseinrichtungen
- Security Compliance Checking
- *Monitoring* (= fortlaufende Überwachung der IT-Systeme)
- Permanente Sensibilisierung der Mitarbeiter

### ***Wartung und administrativer Support von IT-Sicherheitseinrichtungen***

Viele IT-Sicherheitseinrichtungen benötigen für ihren effizienten Einsatz ständige Wartung und administrativen Support. Dazu zählen unter anderem die Auswertung und Archivierung von Protokollen, das Erstellen von Backups, die Überprüfung von sicherheitsrelevanten Parametern (z.B. Zugriffsrechte) auf nicht autorisierte Änderungen und das Aktualisieren der Sicherheitssoftware, besonders im Bereich des Virenschutzes. Die nötigen Tätigkeiten sollten nach einem festen Zeitplan und vor allem regelmäßig durchgeführt werden. Eine Dokumentation aller durchgeführten Tätigkeiten ist für die gesamte IT-Sicherheit von großer Bedeutung.<sup>42</sup>

### ***Security Compliance Checking***

Ein Security Compliance Check soll bestimmen, ob die getroffenen Sicherheitsmaßnahmen im Einklang mit der IT-Sicherheitspolitik und dem IT-Sicherheitsplan stehen. Bei Widersprüchen sind nötige Änderungen einzuleiten. Die Konformität mit der IT-Sicherheitspolitik und

---

<sup>40</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 65ff]

<sup>41</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 65]

dem IT-Sicherheitsplan muss zu jedem Zeitpunkt in der Planung, im Betrieb und während der Außerbetriebnahme gewährleistet sein. Security Compliance Checks sollten für neue IT-Systeme oder relevante neue Anwendungen, sowie für bereits bestehende IT-Systeme und Anwendungen nach einer bestimmten in der IT-Sicherheitspolitik festgelegten Zeit oder nach bedeutenden Änderungen durchgeführt werden. Wenn möglich sollten sie auf standardisierten Tests und Checklisten basieren.<sup>43</sup> In Kapitel 3 der vorliegenden Arbeit wird auf Security Compliance Checks näher eingegangen.

### ***Monitoring***

Monitoring ist die fortlaufende Überwachung, ob das IT-System und seine Benutzer das im IT-Sicherheitsplan festgelegte Sicherheitsniveau beibehalten. Änderungen der Bedrohungen, Schwachstellen, zu schützenden Werte und Sicherheitsmaßnahmen können drastische Auswirkungen auf das Gesamtrisiko haben. Aus diesem Grund müssen diese Aspekte ständig überwacht werden.<sup>44</sup>

### **Change Management**

Das Change Management hat die Aufgabe, neue Sicherheitsanforderungen zu erkennen, welche sich aus Veränderungen des IT-Systems ergeben. Dies ist notwendig, da diese Veränderungen große Auswirkungen auf die Gesamtsicherheit haben können. Änderungen des IT-Systems können auch eine neuerliche Risikoanalyse notwendig machen. Sicherheitsrelevante Veränderungen sind:<sup>45</sup>

- Änderungen der Aufgabenstellung oder der Wichtigkeit der Aufgabe in der Organisation
- Räumliche Änderungen
- Änderungen in der Bewertung der eingesetzten IT, der nötigen Vertraulichkeit, Verfügbarkeit oder Integrität
- Änderungen bei Bedrohungen und Schwachstellen

---

<sup>42</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 65f]

<sup>43</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 66f]

<sup>44</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 67f]

<sup>45</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 68]

## **Incident Handling**

Die Reaktion auf Incidents ist ein wichtiger Bestandteil des IT-Sicherheitsmanagement-Prozesses. Da keine absolute IT-Sicherheit existiert, muss bestimmt werden, was im Falle eines Falles geschehen soll. Aus diesem Grund ist sicherzustellen, dass alle Mitarbeiter über die nötigen Aktionen und Meldewege informiert sind. Diese Aktionen werden in einem *IHP* (=Incident Handling Plan) definiert. Eine Option im Incident Handling ist die Einrichtung eines *CERTs* (=Computer Emergency Response Team), welches sich mit Ursachen und Auswirkungen von Incidents befasst.<sup>46</sup>

### **1.6 Überlegungen zur Durchführung einer IT-Sicherheits-Überprüfung**

Im IT-Sicherheitsmanagement-Prozess findet an unterschiedlichen Punkten eine IT-Sicherheits-Überprüfung statt, namentlich bei der Risikoanalyse, Akkreditierung und der Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb. Die Notwendigkeit der Durchführung dieser Aktivitäten ist gegeben. Die Zeitpunkte der Durchführung sind durch die IT-Sicherheitspolitik festgelegt. Jedoch bleibt aus organisatorischer und unternehmenspolitischer Sicht eine Frage offen: Wer soll die Überprüfung durchführen?

Die Frage danach, wer eine IT-Sicherheits-Überprüfung durchführen soll, hängt von vielen Parametern ab. Die Qualifikation der hauseigenen Mitarbeiter, die zu erwartenden Kosten und die Art der IT-Sicherheits-Überprüfung sind die wichtigsten davon. Die zwei grundlegenden Möglichkeiten sind entweder die Durchführung durch die hauseigene IT-(Sicherheits)-Abteilung, oder das Outsourcing (=Beanspruchung einer entsprechenden Dienstleistung) der IT-Sicherheits-Überprüfung. Beide Varianten haben Vor- und Nachteile. Vorteile der Selbstdurchführung sind:

- bessere Kenntnis des Systems durch eigene Mitarbeiter
- kein Zugriff auf das System durch unternehmensfremde Personen
- geringere Kosten

Durch den Einsatz von unternehmenseigenen Mitarbeitern entfällt die Einarbeitungsphase der IT-Sicherheits-Überprüfung, in der Informationen über das System eingeholt werden. Darüber hinaus ist das Risiko einer Produktionsschädigung durch Systemausfälle während der IT-Sicherheits-Überprüfung geringer. Der Zugriff auf das System durch unternehmensfremde

---

<sup>46</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 68f]

Personen wird verhindert. Schlussendlich sind unternehmenseigene IT-Sicherheits-Überprüfungen relativ gesehen mit geringeren Kosten verbunden. Hier darf nicht vergessen werden, dass für eine ausreichende Schulung der Mitarbeiter gesorgt werden muss. Diese ist wiederum mit Kosten verbunden.

Folgende Gründe sprechen für ein Outsourcing der IT-Sicherheits-Überprüfung:

- spezialisierte bzw. zertifizierte Unternehmen bieten entsprechendes Know-How, eine Schulung der eigenen Mitarbeiter entfällt
- die Notwendigkeit der Bildung einer IT-(Sicherheits)-Abteilung für klein- und mittelständische Unternehmen entfällt
- auch Sicherheitsschwächen, die mittels einer internen IT-Sicherheits-Überprüfung nicht zu entdecken sind, werden aufgespürt
- der Nachweis der Sicherheit eines Systems gegenüber Kunden ist glaubwürdiger, wenn eine IT-Sicherheits-Überprüfung durch spezialisierte bzw. zertifizierte Unternehmen durchgeführt wird
- spezialisierte Unternehmen erledigen IT-Sicherheits-Überprüfungen in der Regel schneller, was bei zeitkritischen Problemen sehr relevant sein kann

Die Entscheidung für oder gegen ein Outsourcing der IT-Sicherheits-Überprüfung ist nicht zwingend. Jedes Unternehmen muss sich die Frage nach den Durchführenden einer IT-Sicherheits-Überprüfung abhängig von der Unternehmens- und IT-Sicherheitspolitik selbst beantworten.

### **1.7 Schlussfolgerungen**

Die IT-Sicherheit wird nur durch den kontinuierlichen IT-Sicherheitsmanagement-Prozess sichergestellt. Eine IT-Sicherheits-Überprüfung muss also, um vollständig zu sein, den IT-Sicherheitsmanagement-Prozess auf seine vollständige Umsetzung und seine Effizienz untersuchen. Zu diesem Zweck existieren einige Methodiken, welche Thema des folgenden Kapitels sind.

## 2 Die Methodiken zur IT-Sicherheits-Überprüfung

Der IT-Sicherheitsmanagement-Prozess wird durch Normen und Standards beschrieben. Unternehmen können sich beispielsweise nach ISO/IEC 17799 richten, um eine angemessene IT-Sicherheit zu etablieren. Normen sollen dazu dienen, ein Ziel zu definieren. Die Art und Weise, dieses Ziel zu erreichen, wird jedoch nicht von der Norm definiert. Die heterogene Natur von IT-Systemen macht es mitunter schwierig, Normen zu erfüllen. Dies schafft Bedarf für eine möglichst einfache und effiziente Methodik, in IT-Systemen unterschiedlichsten Aufbaus die Einhaltung der Normen zu erreichen. Aufbauend auf die existierenden Normen haben verschiedene Institute und Organisationen Methoden entwickelt, um das Ziel der Einhaltung dieser Normen zu erreichen. Anhand dieser Methodiken kann auch die vorhandene IT-Sicherheit überprüft werden. Eine Auswahl der wichtigsten Methodiken wird hier ausführlich vorgestellt, gefolgt von einer ergänzenden Darstellung übriger Methodiken.

### 2.1 BSI Grundschutz

Das BSI publiziert seit 1995 das Grundschutzhandbuch. Das GSHB (=Grundschutzhandbuch) empfiehlt Standardsicherheitsmaßnahmen für typische IT-Systeme. Dabei handelt es sich um organisatorische, personelle, infrastrukturelle und technische Maßnahmen für Systeme mit niedrigem bis mittlerem Schutzbedarf, welche als Basis für kritische Systeme dienen können. Für das Prinzip des Grundschutzansatzes vgl. Unterabschnitt 1.2.2 der vorliegenden Arbeit. Das GSHB bildet mittlerweile einen Quasi-Standard, welcher große Verbreitung auch außerhalb des deutschsprachigen Raums erlangt hat. Das GSHB ist somit sowohl in einer deutschen als auch einer englischen Version erhältlich. Es steht kostenlos zur Verfügung. Zu beziehen ist das GSHB als Download als PDF oder Microsoft Word-Dokument unter <http://www.bsi.de/gshb/downloads/index.htm>. Alternativ dazu gibt es eine HTML-Version unter <http://www.bsi.de/gshb/index.htm>. Darüber hinaus besteht die Möglichkeit, eine CD-ROM zu beziehen, auf der das GSHB in Volltext, sowie sämtliche Hilfsmittel enthalten sind.

Das GSHB wird von einer Vielzahl von Unternehmen und Behörden eingesetzt. Registrierte Anwender werden durch einen Newsletter über Änderungen auf dem Laufenden gehalten und regelmäßig über ihre Erfahrungen mit dem GSHB befragt. Die Antworten der Anwender dienen als Input für die ständige Überarbeitung des GSHB. Eine Liste der registrierten Anwender findet man unter [http://www.bsi.de/gshb/deutsch/etc/gshb\\_reg.htm](http://www.bsi.de/gshb/deutsch/etc/gshb_reg.htm).

Das BSI wurde am 1. Januar 1991 gegründet und gehört als Behörde zum Geschäftsbereich des deutschen Bundesministeriums für Inneres. Das BSI ist eine unabhängige, neutrale Stelle für Fragen im Bereich der IT-Sicherheit. Als Behörde in diesem Bereich ist das BSI innerhalb Europas einzigartig. Es übernimmt Aufgaben in verschiedenen Bereichen der IT-Sicherheit, von den wissenschaftlichen Grundlagen der IT-Sicherheit bis hin zu den strategischen Anwendungen. Darüber hinaus stellt es Grundschutzzertifikate für Organisationen aus. Das BSI ist im WWW erreichbar unter: <http://www.bsi.de>.

### **2.1.1 Anwendungsweisen des IT-Grundschutzhandbuchs**

Der IT-Grundschutzansatz hat zum Ziel, eine detaillierte Risikoanalyse einzusparen. Dies gelingt durch die Auswahl von Standardsicherheitsmaßnahmen, welche für ein IT-System von niedrigem bis mittlerem Schutzbedarf ausgewählt wurden, und im Normalfall ein angemessenes Sicherheitsniveau garantieren. So ist es nur notwendig, die für ein IT-System nötigen Schutzmaßnahmen zu identifizieren und konsequent umzusetzen. Der Aufbau folgt einem Bausteinprinzip, um die Anwendung möglichst einfach und universell zu halten. Das GSHB bietet davon abgesehen Hinweise und praktische Umsetzungshilfen für die Methodik der Einführung eines kontinuierlichen und effektiven IT-Sicherheitsmanagement-Prozesses. Darüber hinaus sind Lösungsansätze für verschiedene Aufgabenstellungen der IT-Sicherheit enthalten, beispielsweise für die IT-Sicherheitskonzeption und IT-Sicherheitsrevision. Die verschiedenen enthaltenen Anwendungsweisen des GSHB seien an dieser Stelle beschrieben.

### **IT-Sicherheitsprozess und IT-Sicherheitsmanagement**

Die im GSHB empfohlenen Maßnahmen zur Etablierung eines kontinuierlichen IT-Sicherheitsmanagement-Prozesses dienen als Grundlage für das Ö-IT-SIHB und sind somit in Kapitel 1 der vorliegenden Arbeit umfassend beschrieben. Bei Abweichungen von der an jener Stelle vorgestellten Vorgangsweise wird auf diese hingewiesen.

### **IT-Strukturanalyse**

Für die Anwendung des GSHB ist es notwendig, die Struktur des vorhandenen IT-Verbunds (=Gesamtheit aller infrastrukturellen, organisatorischen, personellen und technischen Kom-

ponenten in einem Anwendungsbereich der Informationsverarbeitung) zu analysieren und zu dokumentieren. Dafür müssen folgende Aspekte berücksichtigt werden:<sup>47</sup>

- Die vorhandene Infrastruktur,
- Die organisatorischen und personellen Rahmenbedingungen für den IT-Verbund,
- Im IT-Verbund eingesetzte vernetzte und unvernetzte IT-Systeme,
- Die Kommunikationsverbindungen zw. den IT-Systemen und nach außen,
- Im IT-Verbund betriebene Anwendungen

Als Ausgangspunkt für eine Strukturanalyse bietet sich der Netzwerktopologieplan an.

### **Schutzbedarfsfeststellung**

Eine Schutzbedarfsfeststellung ermittelt, welcher Schutz für ein IT-System ausreichend und angemessen ist. Hierbei wird für jede verarbeitete Information und jede Anwendung bestimmt, welche Schäden ein Verlust der Sicherheitsaspekte verursachen würde. Dabei sind insbesondere die möglichen Folgeschäden zu betrachten. Basierend auf diesen Erkenntnissen erfolgt eine Einteilung in drei Schutzbedarfskategorien „niedrig bis mittel“, „hoch“ und „sehr hoch“. Diese Einteilung kommt bei der Anwendung der Grundschutzmethode zum Tragen, da sie die nötigen Maßnahmen bestimmt bzw. eine nachfolgende detaillierte Risikoanalyse bei Verwendung eines kombinierten Ansatzes bedingt.<sup>48</sup>

### **Sicherheitskonzeption**

Für die Erstellung eines IT-Sicherheitskonzeptes ist die stark vernetzte Struktur ein Hindernis. Da das IT-System in seiner Gesamtheit betrachtet werden muss, ist es hilfreich, es in logisch getrennte Teile, eben die IT-Verbünde, zu zerlegen. Voraussetzung für die Anwendung des GSHB auf einen IT-Verbund ist die Kenntnis über dessen Struktur, welche beispielsweise aus der zuvor erwähnten Strukturanalyse gewonnen werden kann. Anschließend können in einem Modellierungsschritt die IT-Grundschutzbausteine auf die Komponenten des IT-Verbunds angewendet werden.<sup>49</sup>

---

<sup>47</sup> [Vgl. GSHB, S. 20]

<sup>48</sup> [Vgl. GSHB, S. 21]

<sup>49</sup> [Vgl. GSHB, S. 21]

### **Basis-Sicherheitscheck**

Der Basis-Sicherheitscheck dient als Instrument, schnell einen Überblick über das IT-Sicherheitsniveau zu erhalten. Mit Hilfe von Interviews wird festgestellt, wie es für einen bestimmten IT-Verbund in Bezug auf die Umsetzung der IT-Grundschutzmaßnahmen bestellt ist. Für jede relevante Maßnahme wird der Umsetzungsstatus als „entbehrlich“, „ja“, „teilweise“ oder „nein“ bestimmt. So kann man noch nicht umgesetzte IT-Grundschutzmaßnahmen identifizieren und so Verbesserungsmöglichkeiten aufzeigen.<sup>50</sup>

### **IT-Sicherheitsrevision**

Die IT-Grundschutzmaßnahmen, welche im GSHB beschrieben werden, können auch für eine IT-Sicherheitsrevision genutzt werden. Zu diesem Zweck sind Checklisten auf Grundlage der IT-Grundschutz-Bausteine für „Organisation“, „Personal“, „PC unter Windows NT“ und „PC unter Windows 95“ entwickelt worden. Sie sind auf der CD-ROM zum GSHB enthalten.<sup>51</sup>

### **Ergänzende Sicherheitsanalyse**

Ergänzende Sicherheitsanalysen können für Systeme mit ermitteltem Schutzbedarf „hoch“ oder „sehr hoch“ angebracht sein. Dabei können verschiedene Methoden angewendet werden, wie die Risikoanalyse, der Penetrationstest und die Differenz-Sicherheitsanalyse.<sup>52</sup> Die Durchführung einer Risikoanalyse wurde in Abschnitt 1.2 der vorliegenden Arbeit erläutert. Penetrationstests werden später in der vorliegenden Arbeit genau behandelt. Eine Beschreibung der Differenz-Sicherheitsanalyse findet sich in der Beschreibung der Anwendung der Grundschutzmethode ebenfalls später in diesem Kapitel.

### **Umsetzung von IT-Sicherheitskonzepten**

Eine angemessene IT-Sicherheit lässt sich nur erreichen, wenn die in der Sicherheitsanalyse gefundenen Schwachstellen durch ein IT-Sicherheitskonzept behandelt werden. Dies steht und fällt natürlich mit der Umsetzung dieses IT-Sicherheitskonzept. Das GSHB liefert Hinweise und Verfahrensweisen für diesen Vorgang.<sup>53</sup>

---

<sup>50</sup> [Vgl. GSHB, S. 21]

<sup>51</sup> [Vgl. GSHB, S. 21f]

<sup>52</sup> [Vgl. GSHB, S. 22]

<sup>53</sup> [Vgl. GSHB, S. 22]

## **Qualifizierung nach IT-Grundschutz**

Durch die weite Verbreitung des IT-Grundschutzansatzes wird dieser in zunehmendem Maße als Quasi-Standard der IT-Sicherheit verwendet. So kann das GSHB verwendet werden, um die vorhandene IT-Sicherheit in einer Organisation zu bewerten. Dies geschieht durch eine IT-Grundschutz-Qualifizierung. Diese dokumentiert, in welcher Form der IT-Grundschutz in der betreffenden Organisation umgesetzt wurde. Zu diesem Zweck wird ein Schema definiert, welches das Qualifizierungsniveau in drei Güteklassen einteilt.<sup>54</sup> Dieses Thema kommt in Folge detaillierter zur Sprache.

### **2.1.2 Die IT-Grundschutzmethode und ihre Anwendung**

Abgesehen von den eben beschriebenen Anwendungsweisen für das GSHB bietet das GSHB eine Methode zur Etablierung des IT-Grundschutzes in einer Organisation. Zum Teil kommen beim Einsatz dieser Methode eben jene zuvor beschriebenen Anwendungsweisen zum Einsatz. Das Hauptaugenmerk liegt auf der IT-Grundschutzmethode, weshalb jene Anwendungsweisen des GSHB, welche in der IT-Grundschutzmethode verwendet werden, hier nochmals genauer betrachtet werden. Die Anwendung des GSHB erfolgt in einer Reihe von Schritten, welche in der Folge dargestellt werden. Ergebnis der Anwendung ist ein IT-Sicherheitskonzept, welches den Grundschutzansatz implementiert. Das Vorhandensein eines IT-Sicherheitsmanagement-Prozesses wird in der Folge vorausgesetzt.

In Abbildung 2-1 wird die prinzipielle Vorgangsweise dargestellt.

### **Strukturanalyse**

Die Strukturanalyse dient zur Vorerhebung von Informationen über das gesamte IT-System, welche in der Folge benötigt werden. Sie besteht aus 4 Teilaufgaben:<sup>55</sup>

1. Netzplanerhebung
2. Komplexitätsreduzierung durch Gruppenbildung
3. Erhebung der IT-Systeme
4. Erfassung der IT-Anwendungen und zugehörigen Informationen

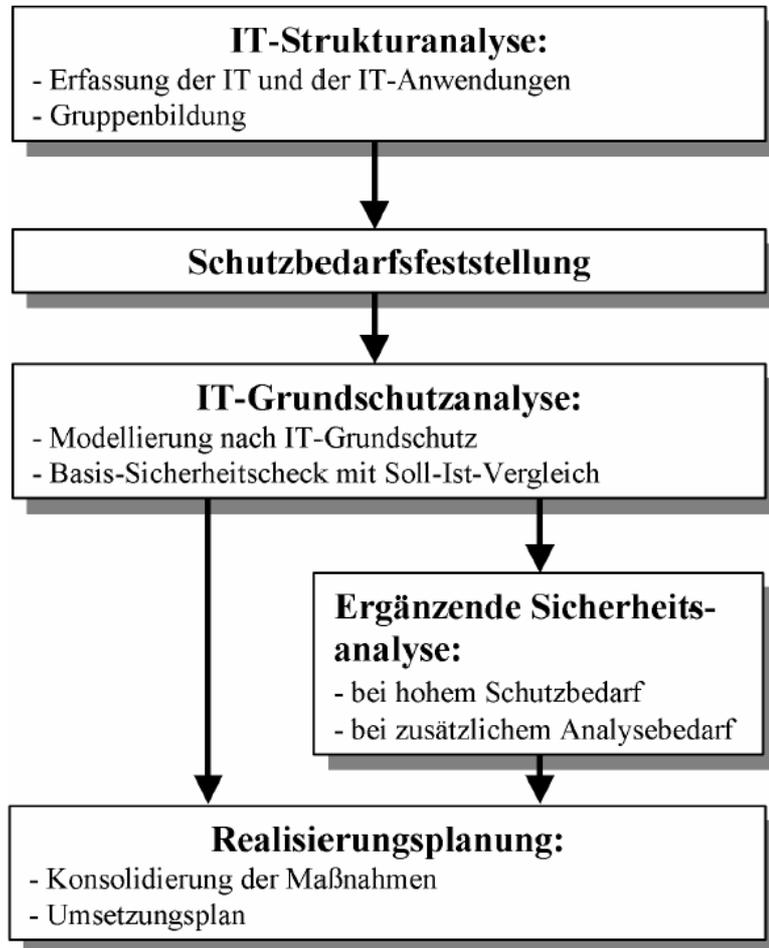
---

<sup>54</sup> [Vgl. GSHB, S. 22]

<sup>55</sup> [Vgl. GSHB, S. 37]

**Netzplanerhebung**

Als Ausgangspunkt für die Strukturanalyse bietet sich ein Topologieplan des Netzwerkes an. Auch im Sinne eines effizienten IT-Sicherheitsmanagements ist es dringend notwendig, einen



**Abbildung 2-1: Erstellung eines IT-Sicherheitskonzeptes nach dem GSHB**

Quelle: GSHB, S. 36

solchen Plan zu erstellen und regelmäßig zu pflegen; d.h. Änderungen in der Netzwerktopologie einzuarbeiten. Folgende Informationen sollten in einem Netzwerktopologieplan enthalten sein:<sup>56</sup>

- IT-Systeme, d.h. Client- und Serverrechner, aktive Netzwerkkomponenten, Netzdrucker, etc.
- Netzverbindungen zwischen diesen IT-Systemen

<sup>56</sup> [Vgl. GSHB, S. 37]

- Verbindungen nach außen, d.h. Dial-Up Verbindungen, Internet-Anbindungen, Funkstrecken oder Mitleitungen zu externen Liegenschaften

Zu jedem dieser Objekte gehören noch einige zusätzliche Informationen aufgelistet. Zumindest enthalten sein sollten:<sup>57</sup>

- Eindeutige Bezeichnung
- Typ und Funktion
- Zugrunde liegende Plattform
- Standort
- Zuständiger Administrator
- Art der Netzanbindung und Netzadresse

Für die Netzanbindungen zwischen den Systemen und nach außen sind folgende Informationen in den Netzwerktopologieplan zu integrieren:<sup>58</sup>

- Art der Verkabelung
- Maximale Datenübertragungsrate
- Verwendete Netzwerkprotokolle (z.B. Ethernet, TCP/IP)
- Bei Außenanbindungen: Details zum externen Netz (z.B. Internet, Name des Providers)

Da in vielen Fällen der Netzwerktopologieplan nicht dem aktuellen Stand entspricht, ist zunächst eine Aktualisierung notwendig.

### ***Komplexitätsreduzierung durch Gruppenbildung***

Als nächsten Schritt erfolgt eine Gruppenbildung von gleichen bzw. gleichartigen Komponenten, die dann jeweils durch ein Objekt repräsentiert werden. Zusammenfassungen von Objekten sind möglich, wenn die einzelnen Komponenten

- vom gleichen Typ sind,
- gleich oder nahezu gleich konfiguriert sind,
- gleich oder nahezu gleich ins Netz angebunden sind,
- den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und
- die gleichen Anwendungen bedienen

---

<sup>57</sup> [Vgl. GSHB, S. 37]

<sup>58</sup> [Vgl. GSHB, S. 37f]

Die Gruppenbildung bedingt, dass Stichproben aus einer Gruppe von Komponenten den IT-Sicherheitsstand der ganzen Gruppe repräsentieren. Beispiele für eine Gruppenbildung sind etwa die Zusammenfassung von Client-Rechnern oder Netzwerkdruckern. Im Anschluss an die Gruppenbildung werden die Gruppen im Netzwerktopologieplan durch ein einzelnes Objekt repräsentiert. Hier ist zu vermerken, wie viele Objekte jeweils zu einer Gruppe zusammengefasst wurden, und von welchem Typ sie sind.<sup>59</sup>

### ***Erhebung der IT-Systeme***

Der nächste Schritt ist die Erhebung der vorhandenen und geplanten IT-Systeme, welche in tabellarischer Form festgehalten werden. Die ist im Hinblick auf die nachfolgende Schutzbedarfsfeststellung und Modellierung des IT-Verbunds wichtig. Als IT-System werden nicht nur Computer im eigentlichen Sinn verstanden, sondern auch aktive Netzwerkkomponenten oder Telekommunikationsanlagen. Hier ist zu beachten, dass sowohl vernetzte als auch nicht vernetzte IT-Systeme erfasst werden. IT-Systeme, welche zuvor zu einer Gruppe zusammengefasst wurden, werden als ein Objekt behandelt. IT-Systeme, welche nicht im Netzwerktopologieplan vermerkt wurden (da sie nicht in das Netzwerk angebunden sind), sind auf eine mögliche Gruppenbildung zu überprüfen. Dies bietet sich vor allem bei einer größeren Menge stand-alone Rechner an.<sup>60</sup>

Für jedes erfasste IT-System sollten folgende Informationen vermerkt sein:<sup>61</sup>

- eindeutige Bezeichnung des IT-Systems,
- Typ und Funktion,
- Plattform (Hardware-Architektur und Betriebssystem)
- Bei Gruppen: Anzahl der zusammengefassten IT-Systeme,
- Aufstellungsort,
- Betriebsstatus (in Betrieb, im Test, in Planung) und
- Anwender/Administrator des IT-Systems

Abbildung 2-2 verdeutlicht das gewünschte Ergebnis anhand eines Beispiels.

---

<sup>59</sup> [Vgl. GSHB, S. 38f]

<sup>60</sup> [Vgl. GSHB, S. 40]

<sup>61</sup> [Vgl. GSHB, S. 40]

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender/Admin.
S1	Server für Personalverwaltung	Windows NT-Server	1	Bonn, R 1.01	in Betrieb	Personalreferat
S2	Primärer Domänen-Controller	Windows NT-Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C1	Gruppe von Clients der Personaldatenverarbeitung	Windows NT-Workstation	5	Bonn, R 1.02 - R 1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Verwaltungsabteilung	Windows NT-Workstation	10	Bonn, R 1.07 - R 1.16	in Betrieb	Verwaltungsabteilung
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in der Außenstelle Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N2	Firewall	Application Gateway auf Unix	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
N3	Switch	Switch	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarbeiter in der Hauptstelle Bonn

**Abbildung 2-2: Erhebung der IT-Systeme**

Quelle: GSBH, S. 41

### *Erfassung der IT-Anwendungen und zugehöriger Informationen*

Es ist nicht notwendig alle auf einem IT-System laufenden Anwendungen zu erfassen. Um die Komplexität dieser Aufgabe möglichst zu reduzieren, ist es ausreichend, wenn zumindest jene Anwendungen erfasst werden, welche jeweils ein Höchstmaß an Vertraulichkeit, Integrität und Verfügbarkeit benötigen. Ihr im Verhältnis zu den restlichen Anwendungen hoher Schutzbedarf deckt somit auch jene restlichen Anwendungen ab. Um sicherzustellen, dass die richtigen Anwendungen erfasst werden, bietet es sich an, die jeweils verantwortlichen Personen und Benutzer zu befragen.<sup>62</sup>

Die Erfassung der IT-Anwendungen wird erleichtert, wenn man sie an den IT-Systemen orientiert zusammenträgt, am besten beginnend mit den Server-Systemen, da diese die größte Wirkung auf das Gesamtsystem ausüben. Weiters ist eine Nummerierung der Anwendungen zweckmäßig. Im Hinblick auf den Datenschutz sollte vermerkt werden, ob die betreffende Anwendung personenbezogene Daten speichert und/oder verarbeitet.

<sup>62</sup> [Vgl. GSHB, S. 41]

Abschließend werden die Anwendungen den IT-Systemen zugeordnet, welche für ihre Ausführung benötigt werden. Dies beinhaltet sowohl die Systeme, auf denen die Anwendung läuft, als auch jene, welche Daten transferieren, die für die Anwendung benötigt werden.<sup>63</sup>

Das Ergebnis der Erhebung ist wiederum eine Tabelle, welche die erhobenen Informationen beinhaltet. Zur Verdeutlichung dient Abbildung 2-3. Ein Eintrag für ein bestimmtes System bei einer bestimmten Anwendung bedeutet, dass das betreffende System für die Ausführung der Anwendung benötigt wird.

Beschreibung der IT-Anwendungen			IT-Systeme						
Anw.-Nr.	IT-Anwendung/Informationen	Pers.-bez. Daten	S1	S2	S3	S4	S5	S6	S7
A1	Personaldatenverarbeitung	X	X						
A2	Beihilfeabwicklung	X	X						
A3	Reisekostenabrechnung	X	X						
A4	Benutzer-Authentisierung	X		X				X	
A5	Systemmanagement			X					
A6	E Xchange (E-Mail, Terminkalender)	X			X				
A7	zentrale Dokumentenverwaltung					X			

**Abbildung 2-3: Erfassung der IT-Anwendungen und zugehöriger Informationen**

Quelle: GSHB, S. 42

### Schutzbedarfsfeststellung

Nachdem die IT-Struktur erfasst wurde, wird eine Schutzbedarfsfeststellung durchgeführt. Diese ist ein wichtiger Schritt in der IT-Grundschutzmethode und gliedert sich in vier Schritte. Zunächst werden die Schutzbedarfskategorien definiert. Danach wird anhand von typischen Schadensszenarien der Schutzbedarf der IT-Anwendungen definiert. Daraus wird der Schutzbedarf für die IT-Systeme abgeleitet. Abschließend wird daraus der Schutzbedarf für die Übertragungsstrecken und Räume abgeleitet.<sup>64</sup>

<sup>63</sup> [Vgl. GSHB, S. 41f]

<sup>64</sup> [Vgl. GSHB, S. 43]

### ***Definition der Schutzbedarfskategorien***

Der Schutzbedarf einer IT-Anwendung bezieht sich auf ihren Schutzbedarf bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Anwendung bzw. der durch sie verarbeiteten Daten. Die Einteilung erfolgt in eine von drei Kategorien. Abbildung 2-4 verdeutlicht dies.

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

**Abbildung 2-4: Schutzbedarfskategorien**

Quelle: GSHB, S. 43

Der Schutzbedarf orientiert sich demnach an den möglichen Schäden, die durch einen Verlust an Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Das GSHB beschreibt sechs Schadenskategorien:<sup>65</sup>

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Außenwirkungen (Image- und Vertrauensverluste)
- Finanzielle Auswirkungen

Häufig treffen mehrere Schadenswirkungen zusammen. Zur Abgrenzung der Schutzbedarfskategorien sollten Grenzen für die einzelnen Schadenskategorien bestimmt werden. So ist beispielsweise ein finanzieller Verlust der Schutzbedarfskategorie „niedrig bis mittel“ für die Organisation tolerabel, einer der Schutzbedarfskategorie „sehr hoch“ hingegen existenzbedrohend.<sup>66</sup> Für die im GSHB definierten Schadensgrenzen siehe Anhang C der vorliegenden Arbeit.

Eventuell ist es angebracht, die Grenzen je nach Organisation anzupassen. Dabei ist zu berücksichtigen, dass die Grundschutzmaßnahmen für die Kategorie „niedrig bis mittel“ ange-

<sup>65</sup> [Vgl. GSHB, S. 43]

bracht sind. Höherer Schutzbedarf bedingt eine ergänzende Sicherheitsanalyse. Die Festlegungen sind jedenfalls im IT-Sicherheitskonzept zu dokumentieren.<sup>67</sup>

### ***Schutzbedarfsfeststellung für IT-Anwendungen***

Nun wird für jede IT-Anwendung untersucht, welche Schutzbedarfskategorie für sie angemessen ist. Dies geschieht unter Zuhilfenahme von Schadensszenarien nach dem Prinzip: Je größer der mögliche Schaden, umso höher der Schutzbedarf.

Das GSHB beschreibt die Erstellung von Schadensszenarien für jede der vorgestellten Schadenskategorien. Auf eine detaillierte Darstellung dieses Vorgangs soll hier verzichtet werden. Die Erstellung der Schadensszenarien erfolgt durch eine Betrachtung der möglichen Auswirkungen eines Schadensfalls einer IT-Anwendung aus der Sicht der Anwender. Um diesen Ablauf zu vereinfachen, stellt das GSHB Fragestellungen für jede der sechs Schadenskategorien zur Verfügung. Sie behandeln jeweils die möglichen Auswirkungen bei Verlust von Vertraulichkeit, Integrität und Verfügbarkeit bezüglich der Schadenskategorie.<sup>68</sup>

Die Ergebnisse dieser Untersuchung werden in einer Tabelle dokumentiert. Sie beinhaltet für jede IT-Anwendung den Grundwert an IT-Sicherheit. Dieser Grundwert bezeichnet den für die IT-Anwendung wichtigsten Aspekt der IT-Sicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit). Darüber hinaus beinhaltet die Tabelle den ermittelten Schutzbedarf und die Begründung dafür, sowie die Information, ob die Anwendung personenbezogene Daten verarbeitet und/oder speichert. Hier kann es auch sinnvoll sein, den Schutzbedarf der IT-Anwendung in Bezug auf den Geschäftsprozess zu dokumentieren. So wird beispielsweise eine Anwendung, die für den Geschäftsprozess unbedingt notwendig ist, in die Schutzbedarfskategorie „sehr hoch“ eingeteilt werden. Dies kann dazu dienen, Fehleinschätzungen der Anwender bei der zuvor durchgeführten Schutzbedarfseinteilung nach oben zu korrigieren.<sup>69</sup>

---

<sup>66</sup> [Vgl. GSHB, S. 44f]

<sup>67</sup> [Vgl. GSHB, S. 46]

<sup>68</sup> [Vgl. GSHB, S. 46ff]

<sup>69</sup> [Vgl. GSHB, S. 52f]

### ***Schutzbedarfsfeststellung für IT-Systeme***

Um den Schutzbedarf der IT-Systeme zu bestimmen, bedient man sich der Informationen, welche zuvor über den Schutzbedarf der IT-Anwendungen gewonnen wurden. IT-Systeme, auf denen Anwendungen mit hohem Schutzbedarf laufen, haben generell ebenfalls höheren Schutzbedarf. Nach dem **Maximum-Prinzip** bestimmt die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf des IT-Systems.<sup>70</sup>

Betrachtet man die Schäden und ihre Auswirkungen, so müssen auch die Abhängigkeiten zwischen den IT-Anwendungen berücksichtigt werden. So dient der Output einer IT-Anwendung oft als Input für eine andere. So kann eine an sich nicht kritische IT-Anwendung an Bedeutung gewinnen, wenn ihr Output für eine kritische IT-Anwendung benötigt wird. Gehören die IT-Anwendungen darüber hinaus noch zu unterschiedlichen Systemen, ist auch eine Schutzbedarfsübertragung zwischen den Systemen nötig. Darüber hinaus ist zu beachten, dass durch die Summe kleinerer Schäden in verschiedenen IT-Anwendungen, welche auf demselben IT-System laufen, ein insgesamt höherer Gesamtschaden entstehen kann (**Kumulationseffekt**). Dies bedingt einen höheren Schutzbedarf des IT-Systems. Auch der umgekehrte Fall ist möglich: Läuft auf einem IT-System eine Anwendung mit hohem Schutzbedarf, so kann es sein, dass sie ihren Schutzbedarf nicht auf das IT-System überträgt, da auf diesem nur unwesentliche Teile der IT-Anwendung ausgeführt werden (**Verteilungseffekt**).<sup>71</sup>

Die Ergebnisse der Schutzbedarfsfeststellung sollten wiederum tabellarisch zusammengefasst werden. Darin wird vermerkt, welchen Schutzbedarf jedes System bezüglich Vertraulichkeit, Integrität und Verfügbarkeit hat. Darüber hinaus findet sich darin die Begründung, welche auch für Außenstehende nachvollziehbar sein muss.<sup>72</sup> Abbildung 2-5 ist ein Beispiel zur Veranschaulichung dieser Ergebnistabelle.

---

<sup>70</sup> [Vgl. GSHB, S. 53]

<sup>71</sup> [Vgl. GSHB, S. 53]

<sup>72</sup> [Vgl. GSHB, S. 54]

IT-System		Schutzbedarfsfeststellung		
Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
S1	Server für Personalverwaltung	Vertraulichkeit	hoch	Maximumprinzip.
		Integrität	mittel	Maximumprinzip.
		Verfügbarkeit	mittel	Maximumprinzip.
S2	Primärer Domänen-Controller	Vertraulichkeit	mittel	Maximumprinzip.
		Integrität	hoch	Maximumprinzip.
		Verfügbarkeit	mittel	Gemäß der Schutzbedarfsfeststellung für Anwendung A4 ist von einem hohen Schutzbedarf für diesen Grundwert auszugehen. Zu berücksichtigen ist aber, dass diese Anwendung auf zwei Rechnersysteme verteilt ist. Eine Authentisierung über den Backup Domänen-Controller in Berlin ist für die Mitarbeiter des Bonner Standortes ebenfalls möglich. Ein Ausfall des Primären Domänen-Controllers kann bis zu 72 Stunden hingenommen werden. Der Schutzbedarf ist aufgrund dieses Verteilungseffekts daher "mittel".

**Abbildung 2-5: Ergebnis der Schutzbedarfsfeststellung für IT-Systeme**

Quelle: GSHB, S. 54

### *Schutzbedarfsfeststellung für Kommunikationsverbindungen*

Anschließend an die Schutzbedarfsfeststellung der IT-Systeme folgt in der Grundschutzmethode die Betrachtung des Schutzbedarfes der Kommunikationsverbindungen. Dieser wird durch mehrere Aspekte bestimmt. Grundlage für die Betrachtung ist der im Vorfeld erstellte Netzwerktopologienplan. Ergebnis ist die Beurteilung, welche Kommunikationsverbindungen redundant ausgelegt bzw. mit kryptographischen Maßnahmen ausgestattet werden sollten, und über welche Angriffe zu erwarten sind. Folgende Kommunikationsverbindungen werden als kritisch eingestuft:<sup>73</sup>

- Außenverbindungen; d.h. Verbindungen die durch oder in unkontrollierte Bereiche (z.B. Internet) führen. Hier besteht die Gefahr, dass bösartige Programme eingespielt

<sup>73</sup> [Vgl. GSHB, S. 55]

werden, Penetrationsversuche durchgeführt werden, oder Innentäter vertrauliche Informationen nach außen übertragen.

- Kommunikationsverbindungen, über die hochschutzbedürftige Informationen übertragen werden. Hier besteht die Gefahr, dass Daten vorsätzlich abgehört und/oder manipuliert werden, bzw. dass IT-Systeme durch Ausfall der Verbindung funktionsunfähig gemacht werden.
- Kommunikationsverbindungen, über die hochschutzbedürftige Informationen nicht übertragen werden dürfen

Die kritischen Kommunikationsverbindungen werden folgendermaßen erfasst: Zunächst werden sämtliche Außenverbindungen erfasst und als kritisch eingestuft. Anschließend folgt die Identifikation jener Verbindungen, die von IT-Systemen mit hohem oder sehr hohem Schutzbedarf ausgehen. Jene, welche zur Übertragung hochschutzbedürftiger Informationen dienen, werden als kritisch eingestuft. Danach untersucht man die Verbindungen, über die diese hochschutzbedürftigen Daten weiterübertragen werden. Abschließend werden jene Kommunikationsverbindungen identifiziert, über die hochschutzbedürftige Daten nicht übertragen werden dürfen. Zu erfassen ist dabei:<sup>74</sup>

- Die Verbindungsstrecke,
- Ob es sich um eine Außenverbindung handelt,
- Ob hochschutzbedürftige Informationen übertragen werden und ob der Schutzbedarf aus der Notwendigkeit für Vertraulichkeit, Integrität oder Verfügbarkeit resultiert und
- Ob hochschutzbedürftige Informationen nicht übertragen werden dürfen

Die erfassten Daten können tabellarisch oder grafisch im Netzwerktopologieplan dargestellt werden.

Besonders wichtig bei dieser Betrachtung ist, dass sie vollständig ist. Nur eine übersehene Kommunikationsverbindung kann die Gesamtsicherheit empfindlich beeinträchtigen. Dies beinhaltet insbesondere Modemverbindungen nach außen, welche den Verantwortlichen unbekannt sind.<sup>75</sup>

---

<sup>74</sup> [Vgl. GSHB, S. 55]

<sup>75</sup> [Vgl. GSHB, S. 57]

***Schutzbedarfsfeststellung für IT-Räume***

Der Schutzbedarf der IT-Räume ergibt sich aus dem Maximum-Prinzip der in dem betreffenden Raum aufgestellten IT-Systeme. Zusätzlich kommt ein möglicher Kumulationseffekt zum Tragen, wenn sich mehrere IT-Systeme in einem Raum befinden. Grundsätzlich ist jeder Raum zu erfassen, in welchem ein IT-System aufgestellt ist. Zu dokumentieren sind sämtliche schutzbedürftige IT-Räume und die Begründung für ihren Schutzbedarf, am besten in tabellarischer Form.<sup>76</sup> Abbildung 2-6 dient wiederum der Veranschaulichung.

Raum			IT	Schutzbedarf		
Bezeichnung	Art	Lokation	IT-Systeme / Datenträger	Vertraulichkeit	Integrität	Verfügbarkeit
R U.02	Datenträger-archiv	Gebäude Bonn	Backup-Datenträger (Wochen-sicherung der Server S1 bis S5)	hoch	hoch	mittel
R B.02	Technikraum	Gebäude Bonn	TK-Anlage	mittel	mittel	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	hoch	mittel
R 1.02 - R 1.06	Büroräume	Gebäude Bonn	C1	hoch	mittel	mittel
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	mittel
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	mittel	hoch	hoch
R 2.01 - R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	mittel	mittel	mittel

**Abbildung 2-6: Ergebnis der Schutzbedarfsfeststellung für IT-Räume**

Quelle: GSHB, S. 57

***Interpretation der Ergebnisse der Schutzbedarfsfeststellung***

Die Ergebnisse der Schutzbedarfsfeststellung sind im Hinblick auf die Modellierung des IT-Grundschatzes wichtig. Je nach Schutzbedarfskategorie sind die Grundschutzmaßnahmen ausreichend oder nicht. Grundsätzlich gilt, dass die Grundschutzmaßnahmen einem Schutzbedarf „niedrig bis mittel“ entsprechen und bei höherem Schutzbedarf eine zusätzliche Sicherheitsanalyse notwendig ist. Bei hohem bis sehr hohem Schutzbedarf sind jedenfalls die im Maßnahmenkatalog als „optional“ gekennzeichneten Maßnahmen zu empfehlen.<sup>77</sup> Abbildung

<sup>76</sup> [Vgl. GSHB, S. 57]

<sup>77</sup> [Vgl. GSHB, S. 58]

2-7 fasst die Schutzwirkungen der Standardsicherheitsmaßnahmen nach IT-Grundschutz zusammen:

Schutzwirkung von Standard-Sicherheitsmaßnahmen nach IT-Grundschutz	
Schutzbedarfskategorie "niedrig bis mittel"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie "hoch"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen können auf Basis einer ergänzenden Sicherheitsanalyse ermittelt werden.
Schutzbedarfskategorie "sehr hoch"	Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, reichen aber alleine i. A. nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden.

**Abbildung 2-7: Schutzwirkung der Grundschutzmaßnahmen**

Quelle: GSHB, S. 58

### Modellierung nach IT-Grundschutz

Nach der Strukturanalyse folgt der eigentliche Hauptteil der IT-Grundschutzmethode, die Modellierung des IT-Verbunds mithilfe der im GSHB beschriebenen Bausteine. Das Ergebnis dieses Vorgangs ist ein IT-Grundschutzmodell des IT-Verbunds. Abhängig davon, ob der IT-Verbund bereits in Betrieb oder noch in Planung ist, dient das IT-Grundschutzmodell des IT-Verbunds als Prüfplan für einen Soll-Ist-Vergleich bzw. als Entwicklungskonzept. Typischerweise ist in einem IT-Verbund beides der Fall. Die Sicherheitsaspekte des IT-Grundschutzes sind in fünf Schichten gruppiert, um die Zuordnung der Bausteine zu erleichtern. Die Sicherheitsaspekte werden den Schichten folgendermaßen zugeordnet:<sup>78</sup>

- Schicht 1 betrifft umfassende Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gelten. Typische Bausteine sind: IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Virenschutzkonzept
- Schicht 2 umfasst die baulich-technischen Gegebenheiten und infrastrukturelle Aspekte der IT-Sicherheit. Typische Bausteine sind: Gebäude, Räume, Schutzschränke und häuslicher Arbeitsplatz
- Schicht 3 betrifft die IT-Systeme des IT-Verbunds, möglicherweise in Gruppen zusammengefasst. Hier werden die Sicherheitsaspekte der Clients und Server sowie der

<sup>78</sup> [Vgl. GSHB, S. 59f]

Stand-alone-Systeme behandelt. Typische Bausteine sind: Unix-System, Tragbarer PC, Windows NT Netz und TK-Anlage

- Schicht 4 betrachtet die Vernetzung und Kommunikation zwischen den IT-Systemen. Typische Bausteine sind: Heterogene Netze, Netz- und Systemmanagement und Firewall
- Schicht 5 schließlich umfasst die eigentlichen IT-Anwendungen, die im IT-Verbund ausgeführt werden. Typischerweise kommen die Bausteine E-Mail, WWW-Server, Faxserver und Datenbanken zum Einsatz

Die Einteilung in Schichten erfolgt aufgrund einiger Vorteile:<sup>79</sup>

- Komplexitätsreduktion der IT-Sicherheit, da Einzelaspekte sinnvoll aufgeteilt und gruppiert werden
- Redundanzen werden vermieden, da Aspekte der niedrigen Schichten nicht nochmals für jedes einzelne System betrachtet werden müssen
- Die Schichten wurden so gewählt, dass auch die Zuständigkeiten für die betrachteten Aspekte gebündelt wurden
- Aufgrund der Schichteneinteilung können Einzelaspekte in resultierenden IT-Sicherheitskonzepten leichter aktualisiert werden, ohne dass andere Schichten berührt werden

Die Modellierung nach IT-Grundschutz ist im Grunde die Entscheidung für die Bausteine einer jeden Schicht, ob und wie sie zur Erstellung des IT-Sicherheitskonzeptes herangezogen werden können. So werden die vorhandenen Bausteine dem Schichtenaufbau folgend auf alle Teile des IT-Verbunds angewendet, auf die sie passen. Diese wichtigen Randbedingungen sind im GSHB für jeden Baustein beschrieben. Beispielsweise ist der Baustein „Windows 2000 Server“ auf alle Server bzw. Servergruppen anzuwenden, auf denen dieses Betriebssystem läuft.<sup>80</sup>

Nachdem alle anzuwendenden Bausteine identifiziert wurden, folgt eine Vollständigkeitsprüfung. Hierbei wird geprüft, ob die Modellierung nach IT-Grundschutz vollständig und ohne Lücken durchgeführt wurde. Wichtig ist hier, dass nicht nur die Hard- und Softwarekomponenten, sondern vor allem auch die organisatorischen, personellen und infrastrukturellen Bausteine angewendet wurden. Um diesen Vorgang zu erleichtern, stellt das GSHB Tabellen zur Verfügung, die für typische Komponenten die unbedingt notwendigen Bausteine auflisten.<sup>81</sup>

---

<sup>79</sup> [Vgl. GSHB, S. 60f]

<sup>80</sup> [Vgl. GSHB, S. 61ff]

<sup>81</sup> [Vgl. GSHB, S. 66f]

Für den Fall, dass Komponenten im IT-Verbund existieren, für die keine Bausteine vorhanden sind, bietet das GSHB eine Methode zur Modellierung neuer IT-Komponenten an. Diese orientiert sich an ähnlichen Bausteinen, die in den allermeisten Fällen vorhanden sein sollten. Da für einen schnellen Soll-Ist-Vergleich, der eine IT-Sicherheits-Überprüfung nach Grundschutz darstellt, für jeden Baustein Formblätter geliefert werden, müssen für neue IT-Komponenten eigene Erhebungsformulare erstellt werden. Geschieht dies, so sollten die Ergebnisse dem BSI übermittelt werden, damit diese unter Umständen auch anderen Anwendern des GSHB zur Verfügung gestellt werden können.<sup>82</sup>

### **Basis-Sicherheitscheck nach IT-Grundschutz**

Das IT-Grundschutzmodell dient auch als Vergleichswert für einen Basis-Sicherheitscheck. Dieser wird als einfacher Soll-Ist-Vergleich durchgeführt. Als Ausgangspunkt dient die Modellierung des IT-Grundschutzes. Der Basis-Sicherheitscheck besteht aus drei Schritten: organisatorischen Vorarbeiten, Soll-Ist-Vergleich, und Dokumentation der Ergebnisse. Für alle in der Modellierung gewählten Standardsicherheitsmaßnahmen wird geprüft, ob sie ausreichend oder nur unzureichend umgesetzt wurden.<sup>83</sup>

Das GSHB beschreibt die Durchführung eines solchen Basis-Sicherheitschecks in umfassender Weise, und stellt auch passende Hilfsmittel etwa für die Dokumentation der Ergebnisse zur Verfügung. Organisatorische Vorarbeiten, wie das Bestimmen von geeigneten (d.h. für die betrachteten Bausteine zuständigen) Interviewpartnern und die Sichtung von organisationsinternen Regelungen (Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Manuals und "informelle" Vorgehensweisen, die die IT-sicherheitsrelevanten Abläufe regeln), stehen zu Beginn des Basis-Sicherheitschecks. Es wird darauf hingewiesen, dass in manchen Bereichen das Hinzuziehen von zusätzlichen Personen zu den in der Folge stattfindenden Interviews und die Erstellung eines Terminplans von Vorteil sind.<sup>84</sup>

Anschließend wird mittels Interviews und stichprobenartigen Kontrollen die Anwendung eines jeden Bausteines überprüft. Als Ergebnis kommen vier verschiedene Aussagen über den Umsetzungsstatus eines einzelnen Bausteines in Betracht:<sup>85</sup>

---

<sup>82</sup> [Vgl. GSHB, S. 67f]

<sup>83</sup> [Vgl. GSHB, S. 69]

<sup>84</sup> [Vgl. GSHB, S. 69f]

<sup>85</sup> [Vgl. GSHB, S. 70f]

- „entbehrlich“: Die Umsetzung der Maßnahmen ist nicht erforderlich, da die den Maßnahmen zugrunde liegenden Gefährdungen nicht existent bzw. durch andere Maßnahmen entkräftet wurden.
- „ja“: Alle Empfehlungen in der Maßnahme wurden vollständig und wirksam umgesetzt
- „teilweise“: Einige der Maßnahmen sind umgesetzt, andere nicht oder nur teilweise
- „nein“: Die Empfehlungen der Maßnahme sind größtenteils noch nicht umgesetzt

Das GSHB bietet Hilfestellungen bei der Durchführung der Interviews und empfiehlt die Durchführung von Stichproben, um die getroffenen Aussagen zu verifizieren. Die Befragten sollten jedenfalls über den ermittelten Status und die Begründung dieser Entscheidung informiert werden.<sup>86</sup>

Die abschließende Dokumentation der Ergebnisse erfolgt mithilfe der vom BSI bereitgestellten Formulare, welche für jeden existenten Baustein vorliegen. In diesen Formularen kann für jede Maßnahme eines Bausteins das Ergebnis des Soll-Ist-Vergleichs in eine Tabelle eingetragen werden. Dieses Dokumentationsmodell ist hinreichend und umfasst für jede Maßnahme den Umsetzungsgrad, geplanten Zeitraum bis zur Umsetzung, verantwortliche Personen, Kostenschätzung und Platz für Bemerkungen und Begründungen für eine eventuell nur teilweise erfolgte Umsetzung. Die Dokumentation kann auch durch das Grundschutztool, ein spezialisiertes Softwarewerkzeug, welches die Anwendung der Grundschutzmethode erleichtert, durchgeführt werden.<sup>87</sup> Das Grundschutztool wird im Abschnitt 3.3.8 der vorliegenden Arbeit vorgestellt.

### **Ergänzende Sicherheitsanalyse**

Wie bereits erwähnt, sind die IT-Grundschutzmaßnahmen nur für IT-Systeme mit niedrigem bis mittlerem Schutzbedarf ausreichend. Bei höherem Schutzbedarf wird eine ergänzende Sicherheitsanalyse empfohlen. Die Durchführung dieser Analysen wird im GSHB kurz gestreift. Das GSHB unterscheidet zwischen drei ergänzenden Sicherheitsanalysen: der Risikoanalyse, dem Penetrationstest und der Differenz-Sicherheitsanalyse.<sup>88</sup> Die Durchführung einer Risikoanalyse ist in Kapitel 1 der vorliegenden Arbeit beschrieben, der Penetrationstest wird anhand einer Studie des BSI zur Durchführung von Penetrationstests in Abschnitt 3.1 be-

---

<sup>86</sup> [Vgl. GSHB, S. 71]

<sup>87</sup> [Vgl. GSHB, S. 71f]

<sup>88</sup> [Vgl. GSHB, S. 74]

schrieben. Aus diesem Grund wird an dieser Stelle lediglich die Differenz-Sicherheitsanalyse betrachtet.

### ***Differenz-Sicherheitsanalyse***

Bei einer Differenz-Sicherheitsanalyse wird grundsätzlich untersucht, ob und wie die realisierten Maßnahmen den in der Praxis etablierten Maßnahmen für den Schutz hochschutzbedürftiger IT-Systeme entsprechen. In einem ersten Schritt werden die realisierten IT-Sicherheitsmaßnahmen, welche über den IT-Grundschutz hinausgehen oder welche im Maßnahmenkatalog des GSHB als optional gekennzeichnet sind, identifiziert. Danach werden diese Maßnahmen mit den in der Praxis etablierten Musterlösungen verglichen. Hierbei muss beachtet werden, dass die IT-Sicherheitsgrundwerte der Vertraulichkeit, Integrität und Verfügbarkeit entscheidend sind. So können gewisse Maßnahmen den einen Grundwert steigern, einen andern hingegen senken. Zum Vergleich der Schutzmaßnahmen veröffentlicht das BSI sog. Schutzklassenmodelle, in denen für bestimmte IT-Systeme höherwertige Schutzmaßnahmen beschrieben werden. Beispiele dafür sind gepanzerte Kabeltrassen oder der Einsatz von mehrstufigen Firewalls in Verbindung mit IDS.<sup>89</sup>

### **Umsetzung von Sicherheitsmaßnahmen**

Als letzten Punkt beschreibt das GSHB die ordentliche Umsetzung der gewählten Sicherheitsmaßnahmen. Voraussetzung für diese Umsetzung ist der erfolgreiche Abschluss und die Ergebnisse der Strukturanalyse, Schutzbedarfsfeststellung, Modellierung und Basis-Sicherheitscheck, sowie gegebenenfalls die Maßnahmenvorschläge der ergänzenden Sicherheitsanalyse. Planung, Durchführung, Begleitung und Überwachung der Umsetzung werden beschrieben. Bei nur wenigen umzusetzenden Maßnahmen und unbegrenzten bzw. ausreichend vorhandenen Mitteln ist eine spontane Umsetzung der Maßnahmen möglich. Typischerweise ist es jedoch vonnöten, die Umsetzung gezielt und strukturiert vorzunehmen. Dies geschieht in sechs Schritten.<sup>90</sup>

---

<sup>89</sup> [Vgl. GSHB, S. 75f]

<sup>90</sup> [Vgl. GSHB, S. 77]

### ***Schritt 1: Sichtung der Untersuchungsergebnisse***

Hier findet die Erstellung einer Gesamtsicht der nicht oder nur teilweise umgesetzten Sicherheitsmaßnahmen statt. Sie ergeben sich aus dem Basis-Sicherheitscheck und einer eventuellen ergänzenden Sicherheitsanalyse.<sup>91</sup>

### ***Schritt 2: Konsolidierung der Maßnahmen***

Nun werden zunächst die noch umzusetzenden Sicherheitsmaßnahmen konsolidiert. Falls durch eine ergänzende Sicherheitsanalyse weitere Sicherheitsmaßnahmen identifiziert wurden, so wird geprüft, inwieweit diese die Grundschutzmaßnahmen ersetzen. Gegebenenfalls müssen die Maßnahmen noch an die spezifischen technischen oder organisatorischen Gegebenheiten angepasst werden. Auch die Betrachtung, ob gewählte Sicherheitsmaßnahmen tatsächlich umsetzbar sind bzw. Abläufe der Organisation behindern, findet hier statt.<sup>92</sup>

### ***Schritt 3: Kosten- und Aufwandsschätzung***

In diesem Schritt werden Kosten und Personalaufwand für die Umsetzung einer Maßnahme abgeschätzt. Oft erwirken Einsparungen bei der Technik erhöhten Personalaufwand. Bei nicht ausreichendem Budget sollte das Restrisiko aufgezeigt werden, das durch nicht umgesetzte Maßnahmen entsteht.<sup>93</sup>

### ***Schritt 4: Festlegung der Umsetzungsreihenfolge der Maßnahmen***

Die Umsetzungsreihenfolge der Maßnahmen wird im Grunde durch die den Maßnahmen zugeordnete Priorität festgelegt. Darüber hinaus ergibt sich bei der Umsetzung oft eine logische Reihenfolge, da die eine Maßnahme ohne die andere nicht umgesetzt werden kann. Maßnahmen mit großer Breitenwirkung oder Maßnahmen von Bausteinen mit einer Vielzahl an Maßnahmen sollten bevorzugt behandelt werden? Bausteine mit größerem Einfluss (z.B. Server) sollten ebenfalls vorrangig behandelt werden.<sup>94</sup>

---

<sup>91</sup> [Vgl. GSHB, S. 77]

<sup>92</sup> [Vgl. GSHB, S. 77f]

<sup>93</sup> [Vgl. GSHB, S. 78]

<sup>94</sup> [Vgl. GSHB, S. 79]

### ***Schritt 5: Festlegung der Verantwortlichkeiten***

In diesem Schritt wird festgelegt, wer bis wann welche Maßnahmen umzusetzen hat. Dies vervollständigt den Realisierungsplan.<sup>95</sup>

### ***Schritt 6: Realisierungsbegleitende Maßnahmen***

Überaus wichtig sind Maßnahmen, welche die Realisierung begleiten und unterstützen. Dazu gehören Programme zur Sensibilisierung und Schulung. Zum Abschluss der Realisierung muss geprüft werden, wie die Akzeptanz der Maßnahmen bei den Mitarbeitern ausfällt. Ursachen für fehlende Akzeptanz müssen gefunden und ihnen entgegengewirkt werden.<sup>96</sup>

#### **2.1.3 Laufende Entwicklungen des IT-Grundschutzes**

Die Grundschutzmethode wird laufend aktualisiert und in neuer Version publiziert. Befragungen und Feedback der registrierten Anwender werden in die neuen Versionen eingearbeitet. Neue Bausteine werden mit den laufenden technischen Neuerungen entwickelt. Eigenentwicklungen von Bausteinen durch Organisationen werden vom BSI entgegengenommen und auf eine Einbindung in das GSHB untersucht. Dies stellt sicher, dass die IT-Grundschutzmethode ständig aktuell gehalten wird; ein Umstand, der die Anwendung ungem ein erleichtert.

Auch die zur IT-Grundschutzmethode vorhandenen Hilfsmittel werden ständig weiter- bzw. neu entwickelt. Anwender werden dazu aufgefordert, eigene Entwicklung von Hilfsmitteln der „Interessensgemeinschaft IT-Sicherheit“ zu übermitteln. So wird vermieden, dass ständig das Rad neu erfunden werden muss.

Durch den Einsatz eines Bausteinprinzips wird erreicht, dass die Anwendung des GSHB auf die unterschiedlichsten Umgebungen möglich ist. Die Grundschutzmethode zeichnet sich somit durch eine hohe Adaptionfähigkeit und Aktualität aus.

#### **2.1.4 Zertifizierung nach BSI Grundschutz**

Eine Zertifizierung nach BSI Grundschutz erfolgt in drei Stufen. Zwei davon sind Vorstufen, die dritte ist das eigentliche Zertifikat, welches durch autorisierte Stellen ausgestellt werden kann. Die Vorstufen werden als „Einstiegsstufe“ und „Ausbaustufe“ bezeichnet. Jede Stufe

---

<sup>95</sup> [Vgl. GSHB, S. 79]

benötigt die Umsetzung gewisser Grundschutzmaßnahmen und baut auf die vorhergehenden auf.<sup>97</sup>

## 2.2 Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> - OCTAVE<sup>SM</sup>

Der OCTAVE<sup>SM</sup>-Ansatz bzw. die OCTAVE<sup>SM</sup>-Methode wurden vom CERT/CC entwickelt und 1999 zum ersten Mal veröffentlicht. Sie stellt eine Methode des Risikomanagements dar, und ist für große Unternehmen und Organisationen gedacht. Sie kann auf verschiedenste Organisationen abgestimmt werden. Darüber hinaus existiert eine Variante für klein- und mittelständische Unternehmen. Die Idee hinter OCTAVE<sup>SM</sup> ist die Erkenntnis, dass eine umfassende Risikobewertung nicht nur die technischen Aspekte der IT-Sicherheit betrachten darf. Deshalb geht der OCTAVE<sup>SM</sup>-Ansatz von den globalen organisatorischen Aspekten und Risiken aus, betrachtet danach die Prinzipien des generellen Risikomanagements, und widmet sich abschließend den Risiken der IT-Infrastruktur.

Der OCTAVE<sup>SM</sup>-Ansatz ging aus den Erfahrungen eines IT-Sicherheits-Evaluierungsteams hervor. Experten erstellten bei den durchgeführten IT-Sicherheits-Überprüfungen eine Liste von organisatorischen und technologischen Schwachstellen und Empfehlungen für die Behebung derselben. Dies stellt einen Ansatz dar, welcher auf Schwachstellen fokussiert ist. Hierbei entsteht nun das Problem, den Schwachstellen Prioritäten zuzuweisen, um die Reihenfolge ihrer Behebung festzulegen. Um dieses Problem zu umgehen, beschlossen die Experten des CERT/CC einen neuen Ansatz zu versuchen: die Fokussierung auf Risiken anstelle von Schwachstellen. Um zu entscheiden, welche Schwachstellen zuerst behoben werden sollen, muss die Schwachstelle im Kontext der Aufgaben und Tätigkeiten der betreffenden Organisation betrachtet werden. Schwachstellen mit großen Auswirkungen auf die Tätigkeiten der Organisation stellen ein größeres Risiko dar und sollten somit bevorzugt behoben werden. Ein risikoorientierter Ansatz hilft beim Verständnis, wie IT-Sicherheit die Ziele der Organisation unterstützt und sichert. In diesem Kontext macht eine Suche nach Schwachstellen mehr Sinn als für sich allein. Durch die Betrachtung der Organisationsziele ist es notwendig, Personal der Organisation in die IT-Sicherheits-Überprüfung einzubeziehen. Dies hilft auch dabei, dem Personal der Organisation ein gewisses Gefühl der Verantwortlichkeit zu entwickeln, die gefundenen Schwachstellen auch zu beheben. Aus diesen Erkenntnissen heraus begann die Entwicklung eines selbstgesteuerten Ansatzes der IT-Sicherheits-Überprüfung und –

---

<sup>96</sup> [Vgl. GSHB, S. 79f]

<sup>97</sup> [Vgl. GSHB, S. 82]

Bewertung. Ergebnis dieser Bemühungen war die Veröffentlichung des OCTAVE<sup>SM</sup>-Frameworks im Jahre 1999. Durch Überarbeitung dieses Frameworks entstand die OCTAVE<sup>SM</sup>-Methode. Durch eine Anpassung an kleinere Organisationen entstand darüber hinaus die OCTAVE<sup>SM</sup>-S-Methode. Zu beziehen ist OCTAVE<sup>SM</sup> kostenlos unter <http://www.cert.org/octave/>, zur besseren Implementierung empfiehlt sich allerdings die Lektüre des dort vorgestellten Buches „Managing Information Security Risks: The OCTAVE<sup>SM</sup> Approach“ von Alberts C. J. und Dorofee A. J., erschienen 2002 bei Addison Wesley.

Auf der OCTAVE<sup>SM</sup>-Website befindet sich eine Downloadstatistik für die beiden OCTAVE<sup>SM</sup>-Methoden. Die Anzahl der Downloads beträgt mehr als 8000 für die OCTAVE<sup>SM</sup>-Methode, bzw. mehr als 4000 für die OCTAVE<sup>SM</sup>-S-Methode. Jeweils die Hälfte dieser Downloads erfolgte durch Unternehmen. Die Statistik steht im WWW unter <http://www.cert.org/octave/statistics.html>.

### 2.2.1 Der OCTAVE<sup>SM</sup>-Ansatz

Der OCTAVE<sup>SM</sup>-Ansatz beschreibt die Konzepte, welche hinter einer erfolgreichen IT-Sicherheits-Überprüfung stehen. Er wird durch die OCTAVE<sup>SM</sup> Criteria (=OCTAVE<sup>SM</sup>-Kriterien) definiert. Dieser beschreibt Prinzipien (=Principles), Attribute (=Attributes) und Ergebnisse (=Outputs). Die Grundideen hinter dem OCTAVE<sup>SM</sup>-Ansatz sind die OCTAVE Principles. Sie beschreiben die Philosophie des OCTAVE<sup>SM</sup>-Ansatzes. Die OCTAVE<sup>SM</sup> Principles sind in drei Gruppen angeordnet:<sup>98</sup>

1. Information Security Risk Evaluation Principles
2. Risk Management Principles
3. Organizational and Cultural Principles

Abbildung 2-8 verdeutlicht die Gruppierung der OCTAVE<sup>SM</sup> Principles und zeigt, welche Principles in den jeweiligen Gruppen enthalten sind.

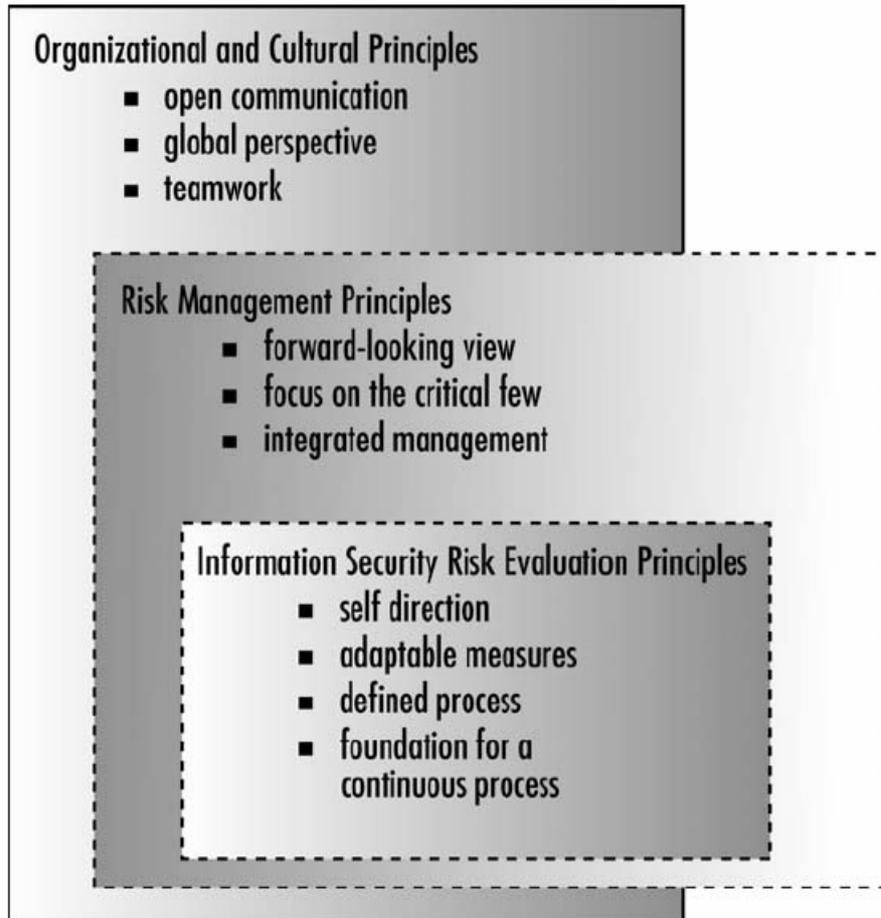
Die Principles beschreiben die Grundlage zur Durchführung einer IT-Sicherheits-Überprüfung gemäß dem OCTAVE<sup>SM</sup>-Ansatz. Wie diese Konzepte in die Durchführung eingearbeitet werden, wird durch die OCTAVE<sup>SM</sup>-Attributes bestimmt. Sie definieren, was notwendig und wichtig ist, um die IT-Sicherheits-Überprüfung zu einem Erfolg - sowohl im Sinne des Prozesses als auch von der organisatorischen Sicht aus - werden zu lassen. Sie sind

---

<sup>98</sup> [Vgl. Alberts & Dorofee 2001, S. 13]

den Principles zuordenbar und zu ihnen konsistent. Die OCTAVE<sup>SM</sup> Outputs definieren die Ergebnisse, welche bei der IT-Sicherheits-Überprüfung erreicht werden müssen.

Die OCTAVE<sup>SM</sup> Principles werden im Folgenden kurz beschrieben. Ebenso wird die Rolle der OCTAVE<sup>SM</sup> Attributes behandelt. Die benötigten OCTAVE<sup>SM</sup> Outputs während der Anwendung der OCTAVE<sup>SM</sup>-Methode werden im folgenden Abschnitt beschrieben.



**Abbildung 2-8: Principles of OCTAVE<sup>SM</sup>**

Quelle: Alberts C. J. und Dorofee A. J. 2001, S. 14

### **Information Security Risk Evaluation Principles<sup>99</sup>**

Diese Principles bilden die Grundlage für eine effektive IT-Sicherheits-Überprüfung.

<sup>99</sup> [Vgl. Alberts & Dorofee 2001, S. 14f]

### ***Self-direction***

Self-direction bezeichnet die Situation, wenn eine IT-Sicherheits-Überprüfung durch organisationseigenes Personal durchgeführt wird. Dies verlangt, dass die Organisation Verantwortung für die IT-Sicherheit übernimmt, indem sie die IT-Sicherheits-Überprüfung durchführt und lenkt, und dass sie Entscheidungen über die zu implementierenden Verbesserungen und Aktionen trifft.

### ***Adaptable Measures***

Adaptable Measures steht für die Notwendigkeit, die in einer IT-Sicherheits-Überprüfung nach OCTAVE<sup>SM</sup>-Ansatz verwendeten Techniken an die technologischen Gegebenheiten anpassen zu können. Dies spiegelt die schnellen Veränderungen in der IT-Sicherheit und der IT allgemein wider. Die IT-Sicherheits-Überprüfung muss demnach flexibel sein. Um dies sicherzustellen, ist es einerseits notwendig, aktuelle Maßnahmenkataloge (=Catalog of Practice) zu haben, die bekannte Sicherheitsmaßnahmen, Bedrohungen und Sicherheitsschwächen beinhalten. Andererseits wird ein IT-Sicherheits-Überprüfungs-Prozess, der sich Änderungen in diesen Katalogen anpassen kann, benötigt.

### ***Defined Process***

Dies steht für die Notwendigkeit einer definierten und standardisierten IT-Sicherheits-Überprüfung. Dies wird erreicht durch:

- Verteilung von Verantwortlichkeiten für die Durchführung der IT-Sicherheits-Überprüfung
- Definition aller Prüfungsaktivitäten
- Benennung aller Werkzeuge, Formblätter und Informationskataloge, welche bei der IT-Sicherheits-Überprüfung verwendet werden
- Erstellung eines gemeinsamen Formats zur Dokumentation der Ergebnisse

### ***Foundation for a Continuous Process***

Das IT-Sicherheitsmanagement muss ein kontinuierlicher Prozess sein. Die Ergebnisse der IT-Sicherheits-Überprüfungen müssen in den Prozess einfließen und Verbesserungen herbeiführen. Ein kontinuierlicher IT-Sicherheitsmanagement-Prozess benötigt:

- Identifizierung der Risiken

- Implementierung der Ergebnisse
- Erstellung der Fähigkeit, kontinuierlich IT-Sicherheitsrisiken zu behandeln
- Implementierung von IT-Sicherheits-Strategien und –Plänen

### **Risk Management Principles<sup>100</sup>**

Diese Principles bilden die Grundlage für effektives Risikomanagement. Sie beziehen sich auf Aspekte, welche den IT-Sicherheits-Überprüfungsprinzipien übergeordnet sind.

#### ***Forward-looking View***

Vorausschauendes Handeln ist essentiell für effektives Risikomanagement. Hauptaugenmerk liegt hierbei auf den kritischsten Unternehmenswerten. Unsicherheiten müssen durch Betrachtung der Werte, Risiken und Schwächen möglichst ausgeschlossen werden.

#### ***Focus on the Critical Few***

Dieses Prinzip beschreibt die Konzentration auf die kritischsten IT-Sicherheitsaspekte. Durch Einschränkungen in Kapital und Personal ist es meist nicht möglich, alle IT-Sicherheitsaspekte gleichermaßen zu behandeln.

#### ***Integrated Management***

Dieses Prinzip nötigt die Organisation, darauf zu achten, dass IT-Sicherheitspolitiken und –strategien mit den allgemeinen Organisationspolitiken vereinbar und konsistent sind. Aus diesem Grund müssen diese bei der Erstellung von IT-Sicherheitspolitiken beachtet werden.

### **Organizational and Cultural Principles<sup>101</sup>**

Dies sind Principles, die für eine funktionierende Organisationskultur sorgen, welche das Risikomanagement unterstützen hilft.

#### ***Open Communication***

IT-Sicherheitsmanagement kann nicht erfolgreich sein, wenn keine offene Kommunikation von IT-sicherheitsbezogenen Themen stattfindet. Offene Kommunikation bedeutet auch,

---

<sup>100</sup> [Vgl. Alberts & Dorofee 2001, S. 16]

<sup>101</sup> [Vgl. Alberts & Dorofee 2001, S. 17f]

dass Meinungen offen geäußert werden dürfen, ohne dass negative Konsequenzen zu erwarten sind. IT-Sicherheitsüberprüfungen bieten oft die Möglichkeit, Meinungen offen äußern zu dürfen. Offene Kommunikation benötigt:

- Prüfungsmethodiken, welche auf gemeinschaftlichen Aktivitäten aufbauen (z.B. Workshops)
- Ermutigung zum Austausch von IT-sicherheitsbezogenen Themen zwischen allen Ebenen der Organisation
- Verwendung von demokratischen Prozessen, welche die individuelle Stimme honorieren

### *Global Perspective*

Dieses Prinzip benötigt, dass die Mitglieder einer Organisation eine gemeinsame Sicht darüber entwickeln, was für die Organisation wichtig ist. Meist gibt es verschiedene Sichtweisen darüber. Es ist nötig, diese Sichtweisen zu identifizieren und sie im größeren Kontext der Organisationsziele zu bewerten.

### *Teamwork*

Teamwork bezeichnet schließlich die Notwendigkeit, die Bewertung der IT-Sicherheit nicht von einem Individuum durchführen zu lassen. Interdisziplinäre Ansätze sind nötig, um technologische und organisatorische Aspekte beiderseits zu betrachten. Die Bildung von interdisziplinären Teams und kooperatives Arbeiten sind deshalb unbedingt erforderlich, um die IT-Sicherheit bewerten zu können.

### **OCTAVE<sup>SM</sup> Attributes<sup>102</sup>**

Die eben betrachteten OCTAVE<sup>SM</sup> Principles bilden die Grundlage des OCTAVE<sup>SM</sup>-Ansatzes. Ihnen sind die 15 OCTAVE<sup>SM</sup> Attributes zuzuordnen, welche bestimmen, wie die Durchführung der IT-Sicherheits-Überprüfung zu den Principles konsistent zu halten ist. Für die Zuordnung der Attributes zu den Principles siehe Anhang D. Eine komplette Beschreibung der OCTAVE<sup>SM</sup> Attributes würde hier zu weit führen, deswegen seien sie hier nur angeführt. Einige davon werden im folgenden Abschnitt bei der Beschreibung der OCTAVE<sup>SM</sup>-Methode beschrieben. Die OCTAVE<sup>SM</sup> Attributes sind:<sup>103</sup>

---

<sup>102</sup> [Vgl. Alberts & Dorofee 2001, S. 19ff]

<sup>103</sup> [Vgl. Alberts & Dorofee 2001, S. 21ff]

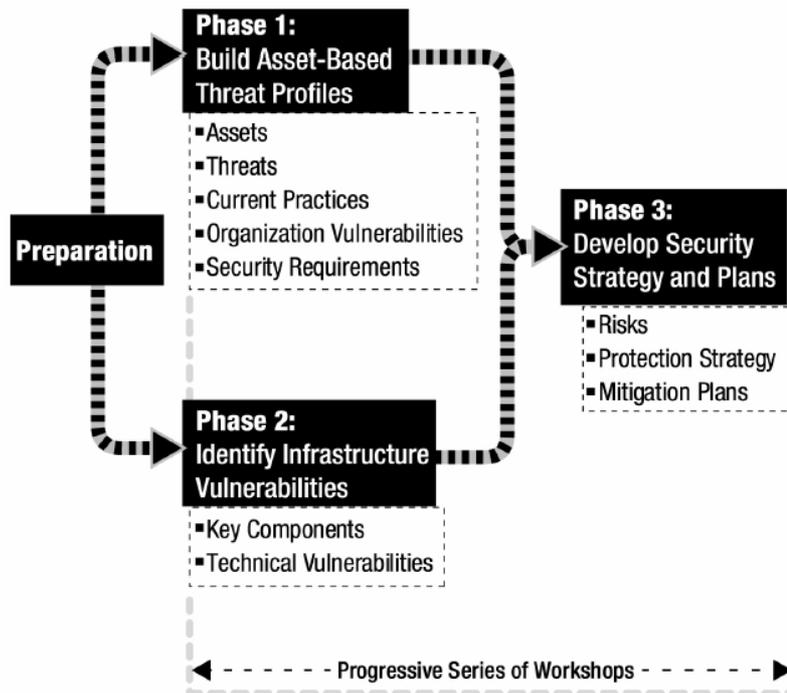
1. Analysis Team
2. Augmenting Analysis Team Skills
3. Catalog of Practices
4. Generic Threat Profile
5. Catalog of Vulnerabilities
6. Defined Evaluation Activities
7. Documented Evaluation Results
8. Evaluation Scope
9. Next Steps
10. Focus on Risk
11. Focused Activities
12. Organizational and Technological Issues
13. Business and Information Technology Participation
14. Senior Management Participation
15. Collaborative Approach

### 2.2.2 Die OCTAVE<sup>SM</sup>-Methode

Die OCTAVE<sup>SM</sup>-Methode zur IT-Sicherheits-Überprüfung folgt einem 3-Phasen-Ansatz und untersucht organisatorische und technologische Aspekte. Sie bildet ein umfassendes Abbild des Bedarfs und Status der IT-Sicherheit innerhalb der Organisation. Jeder der drei Phasen beinhaltet zwei oder mehr Prozesse.<sup>104</sup> Der 3-Phasen-Ansatz und die zu erzielenden Outputs werden in Abbildung 2-9 veranschaulicht.

---

<sup>104</sup> [Vgl. Dorofee, Alberts und Allen 2001, S. 3]



**Abbildung 2-9: Die drei Phasen der OCTAVE<sup>SM</sup>-Methode**

Quelle: Dorofee, Alberts und Allen 2001, S. 3

### OCTAVE<sup>SM</sup> Workshops

Die OCTAVE<sup>SM</sup>-Methode ist workshop-orientiert. Jeder Prozess wird durch einen Workshop, in dem das Analyseteam und gegebenenfalls anderes Personal zusammen arbeiten, durchgeführt. In der OCTAVE<sup>SM</sup>-Methode kommen zwei Arten von Workshops zur Anwendung. Zum einen sind das geführte Diskussionen mit Mitgliedern der Organisation, zum anderen Workshops, in denen das Analyseteam verschiedene Aktivitäten durchführt. Die Organisation der Workshops wird von einem Leiter und einem Schriftführer übernommen. Sie sorgen einerseits für einen geregelten Ablauf und das Einhalten gewisser Principles (z.B. Mehrheitsentscheid), andererseits für die Aufzeichnung der im Workshop erzielten Ergebnisse. Nicht jeder Workshop muss denselben Leiter bzw. Schriftführer haben.<sup>105</sup>

<sup>105</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 3.1]

## Preparation

Zur Vorbereitung auf die Durchführung der OCTAVE<sup>SM</sup>-Methode sind folgende Schritte notwendig:<sup>106</sup>

1. Unterstützung des oberen Managements einholen: Die Unterstützung der Führungsebene der Organisation ist für den Erfolg der IT-Sicherheits-Überprüfung unbedingt erforderlich. Ohne sie ist wenig bis gar keine Unterstützung durch das Personal zu erwarten.
2. Auswahl des Analyseteams: Das Analyseteam spielt als eines der OCTAVE<sup>SM</sup> Attribute eine enorm wichtige Rolle. Es ist für die erfolgreiche Durchführung der IT-Sicherheits-Überprüfung verantwortlich. Ausreichende Fähigkeiten und Training sind für die Mitglieder des Teams verbindlich. Auch das Wissen über die Grenzen der eigenen Fähigkeiten ist wichtig, um bei Bedarf zusätzliche Personen hinzuzuziehen.
3. Bestimmung des angebrachten Horizonts der IT-Sicherheits-Überprüfung: Zu weiter Horizont führt dazu, dass es schwierig wird, alle Informationen zu analysieren. Zu enger Horizont führt hingegen zu wenig aussagekräftigen Resultaten. Das OCTAVE<sup>SM</sup> Principle „focus on the critical few“ kommt hier zum Tragen.
4. Auswahl der Teilnehmer: Während der ersten drei Prozesse der OCTAVE<sup>SM</sup>-Methode steuern Mitglieder unterschiedlichster Ebenen der Organisation Informationen bei. Je nachdem, welcher Prozess durchgeführt wird, sind unterschiedliche Teilnehmer empfohlen. Die Auswahl dieser Personen sollte nach Fähigkeiten und Wissen, nicht nach Verfügbarkeit geschehen. Empfehlungen für die Auswahl sind in der OCTAVE<sup>SM</sup>-Literatur vorhanden.<sup>107</sup>

### Phase 1: Build Asset-Based Threat Profiles<sup>108</sup>

Organisationen stehen immer vor dem Problem, nicht uneingeschränktes Personal bzw. Mittel in die Verbesserung der IT-Sicherheit investieren zu können. Aus diesem Grund ist es interessant herauszufinden, wie man die vorhandenen Mittel am effektivsten einsetzen kann. Der erste Schritt um dies zu erreichen, ist herauszufinden, was für die Organisation wichtig ist und was bereits getan wird, um zu schützen, was für wichtig gehalten wird. Der beste Weg herauszufinden, was in einer Organisation vorgeht, ist die dort tätigen Personen zu befragen. Hier setzt Phase 1 der OCTAVE<sup>SM</sup>-Methode mit einer Folge von Befragungs-Workshops ein. Personal aus verschiedenen Ebenen der Organisation kommt zu Wort und erhält die Möglichkeit, sein jeweils einzigartiges Wissen und seine einzigartigen Sichtweisen aufzuzeigen. Jeder Workshop hat eine unterschiedliche Organisationsebene als Zielgruppe und verwendet Brainstormingstechniken. Die Prozesse der Phase 1 sind mit ihren In- und Outputs in Abbil-

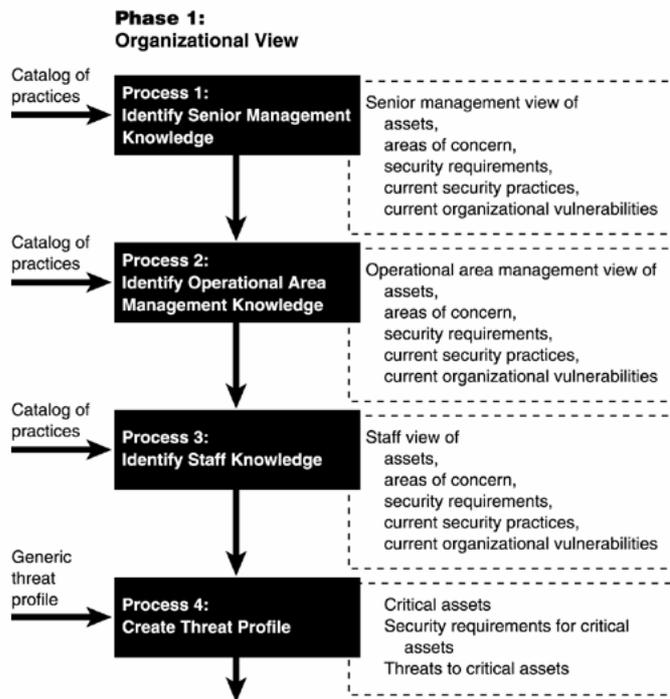
---

<sup>106</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 3.1.1]

<sup>107</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 4.5]

<sup>108</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 5.1]

dung 2-10 dargestellt. Die Prozesse 1 bis 3 beinhalten jeweils dieselben Aktivitäten, die Teilnehmer der Workshops sind jedoch unterschiedlich.



**Abbildung 2-10: Die OCTAVE<sup>SM</sup> Methode: Phase 1**

Quelle: Alberts & Dorofee 2002, Abschnitt 3.1.2

### *Process 1-3: Identify Organization Staff Knowledge<sup>109</sup>*

Folgende Aktivitäten finden in den Prozessen 1-3 statt:

- Identifikation der Unternehmenswerte und relativer Prioritäten
- Identifikation der Problembereiche
- Identifikation der IT-Sicherheitsanforderungen der Unternehmenswerte
- Festhaltung der aktuellen IT-Sicherheitsmaßnahmen und organisatorischer Schwachstellen

Diese vier Aktivitäten werden jeweils mit allen Schichten der Organisation (oberes Management bis Personal) durchgeführt. Als Input dient hierbei der Catalog of Practices.

<sup>109</sup> [Vgl. Alberts & Dorofee 2002, Kap. 5]

Unternehmenswerte sind in diesem Kontext IT-Systeme, Software, Information, Hardware und Personal. Es ist hierbei zu erwarten, dass das Management andere Unternehmenswerte erkennt und als wichtig erachtet als das Personal.

Die Identifikation der Problembereiche ermöglicht das Erkennen von Bedrohungen aus der Sicht der Teilnehmer des Workshops. Dadurch, dass diese über ihren Unternehmensbereich bescheid wissen, lassen sich Probleme erkennen, die andernfalls verborgen blieben. Die Teilnehmer sollen die Problembereiche beschreiben und die möglichen Auswirkungen auf die Unternehmenswerte darstellen.

Sicherheitsanforderungen, welche an die Unternehmenswerte gestellt werden, betreffen die Integrität, Vertraulichkeit und Verfügbarkeit. Diese werden von den Teilnehmern wiederum subjektiv anders bewertet. Hier muss festgehalten werden, welche Anforderungen die Teilnehmer an ihre jeweils wichtigen Unternehmenswerte stellen. Danach wird versucht, diesen Prioritäten zuzuweisen.

Das Festhalten der aktuellen IT-Sicherheitsmaßnahmen und organisatorischer Schwachstellen geschieht mittels eines Fragebogens, der die Vorgänge in der Organisation dem Catalog of Practices gegenüberstellt. Der Aufbau des Fragebogens ist einfach; lediglich „ja“, „nein“ und „weiß nicht“ stehen als Antworten zur Verfügung. Eine anschließende, geführte Diskussion lässt Informationen aufscheinen, die allein durch die Fragebögen nicht ersichtlich wären.

### ***Process 4: Create Threat Profiles<sup>110</sup>***

Prozess 4 besteht aus zwei wichtigen Teilbereichen. Zuerst werden die während den Prozessen 1-3 gesammelten Informationen zusammengefasst und zur Analyse vorbereitet. Dabei sollten etwaige Lücken ersichtlich werden. Danach werden die Daten analysiert. Aus den individuellen Sichtweisen entsteht somit eine globale Perspektive der Unternehmenswerte und Schutzmaßnahmen.

Prozess 4 ist wichtig, da er den Horizont der restlichen IT-Sicherheits-Überprüfung nach OCTAVE<sup>SM</sup> bestimmt. Kritische Unternehmenswerte bestimmen die Infrastrukturbewertung in Phase 2, die Bedrohungsprofile (=Threat Profiles) dienen als Basis für die Risikoanalyse in Phase 3.

---

<sup>110</sup> [Vgl. Alberts & Dorofee 2002, Kap. 6]

Folgende Aktivitäten finden im Prozess 4 statt:

- Zusammenfassung und Gruppierung der gesammelten Informationen
- Auswahl der kritischen Unternehmenswerte
- Verfeinerung der Sicherheitsanforderungen für kritische Unternehmenswerte
- Identifikation der Bedrohungen für kritische Unternehmenswerte

Das generische Bedrohungsprofil (=Generic Threat Profile) ist eines der OCTAVE<sup>SM</sup> Attributes und steht im Mittelpunkt von Prozess 4. Ein Bedrohungsprofil ist eine vom generischen Bedrohungsprofil abgeleitete, strukturierte Art, die Bedrohungen darzustellen, die auf einen Unternehmenswert zutreffen. Bedrohungen werden in der OCTAVE<sup>SM</sup> Methode durch folgende Attribute klassifiziert:

- Asset: der bedrohte Unternehmenswert
- Actor: wer oder was die Sicherheitskriterien eines Unternehmenswertes bedroht
- Motive: ob Absicht hinter der Bedrohung steht oder nicht
- Access: wie der Actor auf den bedrohten Unternehmenswert zugreift (über das Netzwerk oder direkter physikalischer Zugriff)
- Outcome: die unmittelbare Folge der Verletzung von Sicherheitskriterien (Offenlegung, Veränderung, Zerstörung, Verlust, Unterbrechung)

Zur Darstellung der Bedrohungsprofile werden Bedrohungsbäume (=Threat Trees) benutzt. Diese werden in Anhang E aufgeführt.

### *Zusammenfassung der Ergebnisse aus den Prozessen 1 bis 3<sup>111</sup>*

Die Ergebnisse der vorhergehenden Prozesse müssen für den Prozess 4 aufgearbeitet und analysiert werden. Dies geschieht durch eine Gruppierung der Unternehmenswerte, Sicherheitserfordernisse und Areas of Concern (=Bereiche, die von den Befragten als bedroht eingestuft wurden) nach organisatorischer Ebene und Unternehmenswert. Dies macht die Informationen leichter les- und verwertbar.

### *Auswahl der kritischen Unternehmenswerte<sup>112</sup>*

Dieser Schritt ist für die IT-Sicherheits-Überprüfung nach der OCTAVE<sup>SM</sup>-Methode maßgeblich. Durch die Befragung der Mitarbeiter der Organisation wird erwartungsgemäß eine

---

<sup>111</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 6.2]

Vielzahl an Unternehmenswerten identifiziert. Bei großen Unternehmen ist eine Einschränkung des Überprüfungshorizonts notwendig, um die IT-Sicherheits-Überprüfung durchführbar zu machen. Aus diesem Grund werden in diesem Schritt die für die Organisation wichtigsten Unternehmenswerte bestimmt. Diese werden in der Folge überprüft. Die Auswahl erfolgt im Rahmen eines weiteren Workshops, der die verschiedenen Meinungen der Teilnehmer zusammenführt. Die OCTAVE<sup>SM</sup>-Methode schlägt die Auswahl der fünf wichtigsten Unternehmenswerte vor, jedoch können auch mehr oder weniger Unternehmenswerte ausgewählt werden.

### *Verfeinerung der Sicherheitsanforderungen für kritische Unternehmenswerte<sup>113</sup>*

In diesem Schritt wird für jeden Unternehmenswert die wichtigste Sicherheitsanforderung bestimmt. Unterschiedliche Sichtweisen der Mitarbeiter müssen unter Verwendung einer organisationsbezogenen Perspektive vereint werden. Betrachtet beispielsweise das Management die Vertraulichkeit eines Unternehmenswertes als wichtigste Sicherheitsanforderung, das Personal jedoch die Verfügbarkeit, muss versucht werden, das Problem aus der ganzheitlichen Sicht der Organisation zu betrachten. Dies kann ein schwieriges Problem darstellen. Grundsätzlich werden in diesem Schritt die Sicherheitsanforderungen jedes Unternehmenswertes beschrieben und Prioritäten zugewiesen.

### *Identifikation der Bedrohungen für kritische Unternehmenswerte<sup>114</sup>*

Nachdem nun untersucht wurde, welches die kritischen Unternehmenswerte sind, und welche Sicherheitsanforderungen die wichtigsten sind, wird untersucht, wie diese Unternehmenswerte bzw. Sicherheitsanforderungen bedroht sind. In diesem Schritt wird für jeden kritischen Unternehmenswert ein Bedrohungsprofil erstellt. Für jeden der kritischen Unternehmenswerte wird bestimmt, welche Bedrohungen zutreffend bzw. vernachlässigbar sind. Dies geschieht unter Zuhilfenahme der Bedrohungsbäume (s. Anhang E). Ergebnis ist die Auflistung aller Bedrohungen für alle kritischen Unternehmenswerte.

### ***Outputs der Phase 1***

Folgende OCTAVE<sup>SM</sup> Outputs müssen als Ergebnis der Phase 1 (Prozesse 1 bis 4) erzielt werden:<sup>115</sup>

---

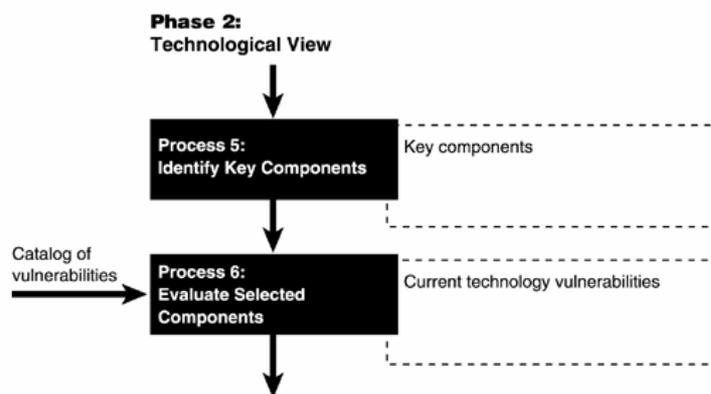
<sup>112</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 6.3]

<sup>113</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 6.4]

- Critical Assets: Kritische Unternehmenswerte
- Security Requirements for Critical Assets: Sicherheitsanforderungen für die kritischen Unternehmenswerte (Integrität, Vertraulichkeit, Verfügbarkeit)
- Threats to Critical Assets: Bedrohungen für kritische Unternehmenswerte
- Current Security Practices: Derzeit eingesetzte Sicherheitsmaßnahmen
- Current Organizational Vulnerabilities: Derzeitige organisatorische Schwachstellen

## Phase 2: Identify Infrastructure Vulnerabilities<sup>116</sup>

Phase 2 der OCTAVE<sup>SM</sup>-Methode widmet sich den technologischen Aspekten der IT-Sicherheit. Sie besteht aus den Prozessen 5 und 6 und wird in Abbildung 2-11 veranschaulicht.



**Abbildung 2-11: Die OCTAVE<sup>SM</sup> Methode: Phase 2**

Quelle: Alberts & Dorofee 2002, Abschnitt 3.1.3

In Prozess 5 erfolgt die Auswahl der technologischen Schlüsselkomponenten, welche in Prozess 6 unter Verwendung von Werkzeugen zur IT-Sicherheits-Überprüfung auf Schwachstellen untersucht werden. Die Schwachstellen, die gefunden werden sollten, können im Design, in der Implementierung und in der Konfiguration liegen.

### *Process 5: Identify Key Components<sup>117</sup>*

Die Ergebnisse von Prozess 4 dienen als Hilfe, wie die IT-Infrastruktur der Organisation auf technologische Schwachstellen untersucht werden soll. Um das Risiko festzustellen, muss

<sup>114</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 6.5]

<sup>115</sup> [Vgl. Alberts & Dorofee 2001, S. 37]

<sup>116</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 3.1.3]

<sup>117</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 7.1]

man sich auf die Schlüsselkomponenten konzentrieren, welche für die kritischen Unternehmenswerte relevant sind. Prozess 5 ermöglicht die Auswahl dieser Schlüsselkomponenten. Zwei Aktivitäten finden im Prozess 5 statt:

- Identifizierung der Schlüsselklassen von Komponenten
- Identifizierung der zu untersuchenden Infrastrukturkomponenten

Zuerst werden die für einen kritischen Unternehmenswert wichtigen Klassen von Komponenten bestimmt. Dies sind jene, welche den Zugriff auf die Unternehmenswerte ermöglichen. Danach wird nach dem OCTAVE<sup>SM</sup> Principle „Focus on the Critical Few“ bestimmt, welche Komponenten die kritischsten für den Unternehmenswert sind. Diese werden überprüft. Für die Durchführung der Aktivitäten ist ein Netzwerktopologieplan nötig.

### *Identifizierung der Schlüsselklassen von Komponenten<sup>118</sup>*

Hier wird für jeden Unternehmenswert zuerst das sogenannte „System of Interest“ bestimmt. Dieses ist jenes System, welches einem Angreifer den Zugriff auf den betreffenden Unternehmenswert ermöglicht. Als Ausgangspunkt dient hierbei der Bedrohungsbaum für menschliche Akteure mittels Netzwerkzugriff. Darin sind jegliche Bedrohungen in diesem Kontext aufgezeigt. Mittels des Netzwerktopologieplans sollte es möglich sein, das System of Interest eines jeden Unternehmenswertes zu bestimmen. Es ist auch möglich, dass es mehrere Systems of Interest gibt. Danach werden die Schlüsselklassen der Komponenten bestimmt, welche Teile des System of Interest sind oder mit ihm in Verbindung stehen. Dies sind jene Komponenten, welche autorisierten bzw. unautorisierten Benutzern den Zugriff auf das System of Interest ermöglichen. Hilfreich dafür ist die Erstellung von Zugriffspfaden mittels Netzwerktopologieplan. Alle Systeme, welche im Zugriffspfad zum System of Interest enthalten sind, sind Schlüsselklassen von Komponenten für dieses System of Interest. Beispiele dafür sind Server, Desktoprechner, Drahtlose Geräte, Sicherheitskomponenten (z.B. Firewall), Notebooks, Handhelds, Mobiltelefone oder Heimcomputer. In der folgenden Aktivität werden spezifische Komponenten der Schlüsselklassen für eine Überprüfung auf Schwachstellen ausgewählt.

---

<sup>118</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 7.2]

### *Identifizierung der zu untersuchenden Infrastrukturkomponenten<sup>119</sup>*

Die Auswahl der zu untersuchenden Infrastrukturkomponenten muss sicherstellen, dass die Schwachstellenanalyse dieser Auswahl ein Bild der typischen Gefährdung der betreffenden Schlüsselklasse von Komponenten ergibt. Dies erfordert oft die Überprüfung von mehr als einer Komponente jeder Schlüsselklasse. Je typischer eine Komponente für ihre Schlüsselklasse ist, umso geeigneter ist sie für eine Schwachstellenanalyse. Zu beachten ist, ob eine Schwachstellenanalyse eventuell eine Komponente außer Betrieb setzen und den Produktionsprozess unterbrechen könnte. Dies könnte besondere Erlaubnis oder Zeitplanung voraussetzen. Die ausgewählten Komponenten sind mit ihrer Netzwerkadresse und vollständigen Hostnamen, sowie dem Grund ihrer Auswahl zu dokumentieren. Für alle kritischen Unternehmenswerte ist für jeweils alle Schlüsselklassen ihrer Systems of Interest mindestens eine Komponente auszuwählen. Da manche Komponenten für mehr als einen kritischen Unternehmenswert relevant sind, ist es sinnvoll, nach Redundanzen zu suchen.

Das Ziel der Auswahl ist es, ein Gefühl für die Verwundbarkeit der Schlüsselklassen von Komponenten zu bekommen. Die Entscheidung, wie viele Komponenten einer jeden Schlüsselklasse auszuwählen sind, wird nicht reglementiert. Dies muss das Analyseteam jeweils selbst entscheiden.

Nach der Auswahl der Komponenten zur Schwachstellenanalyse folgt die Entscheidung für einen bestimmten Ansatz der Schwachstellenanalyse. Hier stellt sich die Frage, ob ein Outsourcing der Schwachstellenanalyse angebracht ist, oder ob diese durch internes Personal durchgeführt werden soll. Darüber hinaus muss entschieden werden, welche Werkzeuge bei der Schwachstellenanalyse zum Einsatz kommen. Dies beinhaltet Software und Checklisten. Eine Auswahl der hier verwendbaren Werkzeuge wird in Abschnitt 3.3 der vorliegenden Arbeit vorgestellt.

### ***Process 6: Evaluate Selected Components<sup>120</sup>***

Der Prozess 6 ist einzigartig innerhalb der OCTAVE<sup>SM</sup>-Methode, da vor dem Workshop eine große technische Aufgabe steht: die Schwachstellenanalyse der gewählten Komponenten. Welche Komponenten das sind und wie und von wem die Schwachstellenanalyse ausgeführt wird, wurde im vorangegangenen Prozess entschieden. Die Ausführenden der Schwachstel-

---

<sup>119</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 7.3]

lenanalyse müssen die Ergebnisse dokumentieren und dem Analyseteam vor dem Workshop aushändigen. Während des Workshops werden diese Ergebnisse dann betrachtet und analysiert.

Die Vorbereitung auf die Schwachstellenanalyse umfasst die Vorbereitung der ausgewählten Werkzeuge (aktuelle Versionen bereitstellen) und die Informierung aller betroffenen Personen. Da eine Schwachstellenanalyse unter Umständen den Produktionsprozess gefährden kann, müssen entsprechende Genehmigungen eingeholt werden.

Die Werkzeuge zur Schwachstellenanalyse liefern üblicherweise Reporte ihrer Ergebnisse, in denen die gefundene Schwachstelle genannt und beschrieben wird. Die Schwere der Schwachstelle sowie die nötigen Schritte zu ihrer Behebung werden ebenfalls beschrieben. Diese Reporte werden nun in einer vorläufigen Form zusammengefasst. Für jeden kritischen Unternehmenswert wird aufgelistet, welche Schwachstellen vorhanden sind, und wie dringend ihre Behebung ist.

Die Ergebnisse der vorläufigen Zusammenfassung werden im folgenden Workshop betrachtet und gegebenenfalls verändert. Für jeden kritischen Unternehmenswert muss bekannt sein, welche Schwachstellen auf ihn zutreffen, wie dringend die Behebung dieser Schwachstellen ist, welche potentiellen Folgen die Schwachstellen haben, und wie die Schwachstellen behoben werden können. Gegebenenfalls können die Dringlichkeiten der Behebung verändert werden. Ergebnis dieses Workshops sind die nötigen Aktionen und Empfehlungen zur Behebung der Schwachstellen. Alle Ergebnisse müssen sorgfältig dokumentiert sein, um später die Formulierung der Schutzstrategien in Prozess 8 zu erleichtern.

Nachdem die Informationen über die technologischen Schwachstellen der kritischen Unternehmenswerte bekannt sind, wird auf das in Prozess 4 erstellte Bedrohungsprofil zurückgegriffen und überprüft, ob neue Bedrohungen offenkundig wurden. Neue Bedrohungen müssen im Bedrohungsprofil markiert werden.

### ***Outputs der Phase 2***

Folgende OCTAVE<sup>SM</sup> Outputs müssen als Ergebnis der Phase 1 (Prozesse 1 bis 4) erzielt werden:<sup>121</sup>

---

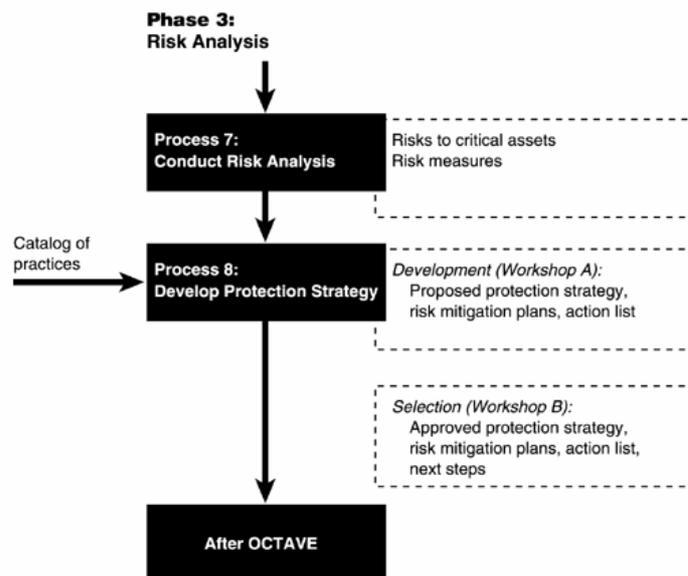
<sup>120</sup> [Vgl. Alberts & Dorofee 2002, Kap. 8]

<sup>121</sup> [Vgl. Alberts & Dorofee 2001, S. 37]

- Key Components: Schlüsselkomponenten der kritischen Unternehmenswerte
- Current Technology Vulnerabilities: derzeitige technologische Schwachstellen, durch ein Werkzeug zur Schwachstellenanalyse identifiziert

### Phase 3: Develop Security Strategy and Plans<sup>122</sup>

Phase 3 der OCTAVE<sup>SM</sup>-Methode beschäftigt sich mit der Risikoanalyse und den Strategien zur Risikomilderung. Risiken, welche die kritischen Unternehmenswerte betreffen, entstehen durch das Zusammenwirken der Schwachstellen und der möglichen Folgen. Um diese Risiken zu bewerten, beschäftigt sich das Analyseteam in Phase 3 mit den möglichen Auswirkungen eines Angriffs auf einen kritischen Unternehmenswert. Dies geschieht nicht nur in Anbetracht der unmittelbaren Folgen (z.B. Verlust der Verfügbarkeit eines Systems), sondern im Kontext der Ziele und Strategien der Organisation. Nach der Durchführung der Risikoanalyse werden eine Schutzstrategie ausgearbeitet und Pläne zur Milderung der Risiken geschmiedet. Der strukturelle Aufbau von Phase 3 wird in Abbildung 2-12 verdeutlicht.



**Abbildung 2-12: Die OCTAVE<sup>SM</sup>-Methode: Phase 3**

Quelle: Alberts & Dorofee 2002, Abschnitt 3.1.4

Prozess 7 der OCTAVE<sup>SM</sup>-Methode ist die Durchführung einer Risikoanalyse. Ziel der Risikoanalyse ist es, das für einen kritischen Unternehmenswert geltende Risiko zu bestimmen.

<sup>122</sup> [Vgl. Alberts & Dorofee 2002, Kap. 9]

Darauf folgt Prozess 8, der die Schutz- und Risikomilderungsstrategien vorschlägt und anschließend bestätigt. Wie in der obigen Abbildung ersichtlich, besteht Prozess 8 aus zwei Workshops. Die Bestätigung der im ersten Workshop ausgearbeiteten Pläne erfolgt im zweiten Workshop unter Miteinbeziehung des oberen Managements. Nach Abschluss von Prozess 8 ist die OCTAVE<sup>SM</sup>-Methode beendet und es folgt die Implementierung der ausgearbeiteten Strategien.

### ***Process 7: Conduct Risk Analysis***<sup>123</sup>

Eines der OCTAVE<sup>SM</sup> Attributes ist der "Focus on Risk". Dieses Attribut verlangt, das Risiko im Kontext der Ziele und Strategien der Organisation zu betrachten. Bis zu diesem Punkt wurden in der OCTAVE<sup>SM</sup>-Methode Daten gesammelt, um ein Bild der IT-Sicherheits-Bedrohungen zu zeichnen. Prozess 7 befasst sich nun mit den Risiken, welche diese Bedrohungen auf die Organisation erwirken. Folgende Aktivitäten finden in Prozess 7 statt:

- Identifizierung der Impacts (=Auswirkungen von Bedrohungen auf die Organisation) von Bedrohungen auf kritische Unternehmenswerte
- Erstellung von Risikobewertungskriterien
- Bewertung der Impacts von Bedrohungen auf kritische Unternehmenswerte

Zum Verständnis der Risikoanalyseaktivitäten in Prozess 7 ist die in OCTAVE<sup>SM</sup> verwendete Risikodefinition notwendig. Risiko entsteht durch Bedrohungen. Die Wahrscheinlichkeit für das Eintreten eines negativen Ereignisses ist in der Informationstechnologie schwer einschätzbar. In der OCTAVE<sup>SM</sup>-Methode wird eine Methode vorgeschlagen, die Unsicherheit der Risiken auf der Basis von Szenarioplanung zu behandeln.

Was schlussendlich in der Risikobewertung zählt, sind die Impacts, welche die unmittelbaren Folgen einer Bedrohung (=Outcome) haben. Es gibt vier Arten von Outcomes:

- Offenlegung eines kritischen Unternehmenswertes
- Veränderung eines kritischen Unternehmenswertes
- Verlust/Zerstörung eines kritischen Unternehmenswertes
- Unterbrechung eines kritischen Unternehmenswertes

---

<sup>123</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 9.1]

Die Outcomes bezeichnen die Auswirkungen auf den kritischen Unternehmenswert, der Impact hingegen die Auswirkungen auf die Organisation. Sie sind die direkte Verbindung zu den Organisationszielen und –strategien.

### *Identifizierung der Impacts von Bedrohungen auf kritische Unternehmenswerte<sup>124</sup>*

Diese Aktivität stellt die Verbindung zwischen kritischen Unternehmenswerten, Bedrohungen und den Organisationszielen her und schafft die Basis für eine Bewertung der Risiken. Nach einer neuerlichen Betrachtung der in Prozess 4 gesammelten Daten (Sicherheitsanforderungen, Bedrohungsprofile, Areas of Concern) folgt die Betrachtung der möglichen Impacts in folgenden Bereichen:

- Image/Kundenvertrauen
- Sicherheit und Gesundheit
- Bußgelder und gerichtliche Strafen
- Finanzen
- Produktivität

Diese Bereiche müssen gegebenenfalls in Übereinstimmung mit den Organisationszielen ergänzt werden. Ein Beispiel dafür ist der Bereich „Einsatzbereitschaft“ für militärische Organisationen.

Nun wird für jeweils jeden kritischen Unternehmenswert für alle Bedrohungen im Bedrohungsprofil geprüft, ob ein Impact in den oben genannten Bereichen möglich ist. Die Ergebnisse sind genau zu dokumentieren.

### *Erstellung von Risikobewertungskriterien<sup>125</sup>*

Die erste Aktivität tat den ersten Schritt der Überleitung von Bedrohungen auf das Risiko. Nun ist es nötig, Risikotoleranzen für die Organisation zu definieren. Dazu ist eine Bewertung der Risiken nötig, die durch die Erstellung von geeigneten Kriterien ermöglicht wird. Jede Organisation muss Prioritäten zur Milderung von Risiken setzen, da es meist nicht möglich ist, alle Risiken gleichermaßen zu mildern. Zur Prioritätensetzung nimmt man Organisationsziele und –strategien, rechtliche Vorgaben, Standards welche die Organisation einhalten muss, Versicherungsinformationen, und Resultate von anderen Risikomanagementprozessen der Organisation als Entscheidungshilfe. Hier erweist sich das OCTAVE<sup>SM</sup> Principle der Self-

---

<sup>124</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 9.2]

<sup>125</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 9.3]

direction als äußerst sinnvoll, da die Risiken immer aus der Sicht des Unternehmens bewertet werden müssen. Somit müssen die Risikobewertungskriterien immer im Kontext der Organisation erstellt werden.

Nachdem alle relevanten Hintergrundinformationen betrachtet wurden, folgt die Entscheidung, welche Impacts in den jeweiligen Impactbereichen als stark, mittel bzw. schwach einzustufen sind. So kann zum Beispiel ein schwacher Impact im Bereich der Produktivität einen Verlust von drei Tagen bedeuten, ein starker einen Verlust von drei Wochen. Die Ergebnisse dieser Betrachtung sind die Risikobewertungskriterien.

In dieser Methode ist das Maß für das Risiko der Impact. Eine andere Sichtweise im Risikomanagement nimmt die Wahrscheinlichkeit als Maß. In der IT-Sicherheit ist die Wahrscheinlichkeit jedoch schwer handhabbar, da sich die Gegebenheiten sehr schnell verändern und somit gesicherte Daten und Einschätzungen schwer zu erhalten sind. Aus diesem Grund betrachtet OCTAVE<sup>SM</sup> die Bedrohungen und versucht, mithilfe von Szenarioplanung die Bedrohungen mit den schwerwiegendsten Auswirkungen zu mildern. Im Gegensatz dazu behandelt eine wahrscheinlichkeitsorientierte Methode bevorzugt die Bedrohungen mit der höchsten Eintrittswahrscheinlichkeit.

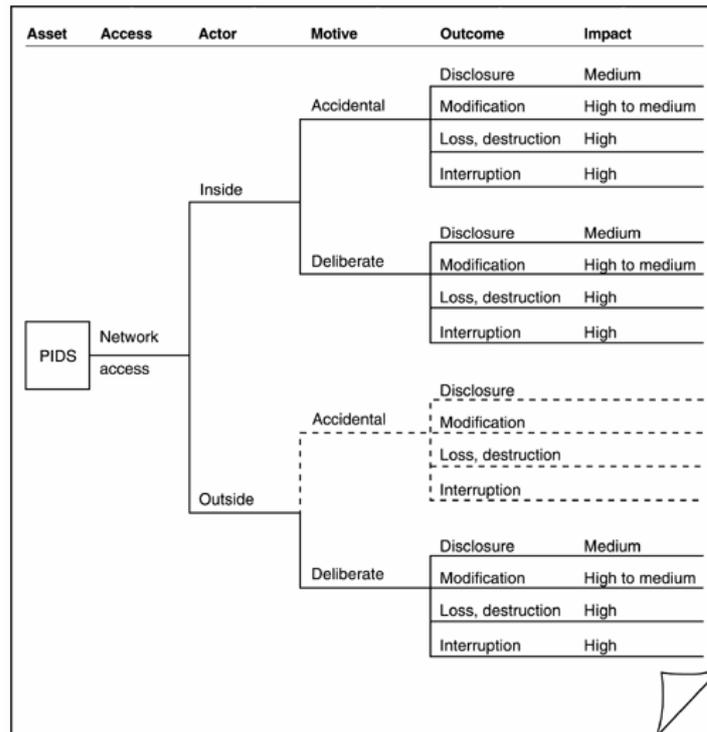
Die Risikobewertungskriterien, die im Laufe dieser Aktivität erstellt wurden, sind ein nützliches Werkzeug, und jedenfalls als Input für zukünftige IT-Sicherheits-Überprüfungen nach der OCTAVE<sup>SM</sup>-Methode verwendbar. Ihre Erstellung ist häufig ein iterativer Prozess und nicht zwingend in Prozess 7 anzusiedeln. Auch eine frühere Erstellung ist denkbar.

### *Bewertung der Impacts von Bedrohungen auf kritische Unternehmenswerte<sup>126</sup>*

Die gefundenen Risikobewertungskriterien müssen nun nur noch auf alle Bedrohungen angewandt werden. Dazu benutzt man die zuvor gesammelten Informationen. Szenarien, welche die kritischen Unternehmenswerte bedrohen (=Bedrohungsprofile), die daraus folgenden Impacts, und die Risikobewertungskriterien bilden gemeinsam ein Bild der IT-Sicherheitsrisiken, denen die Organisation ausgesetzt ist. Dies wird durch eine Bewertung aller Impacts für alle kritischen Unternehmenswerte erreicht. Durch die Zuordnung von Bewertungskriterien zu den Impacts entsteht aus dem Bedrohungsprofil ein Risikoprofil. Ein Beispiel für ein Risikoprofil findet sich in Abbildung 2-13. Durchgezogene Äste des Baumes stellen ein Risiko dar, gestrichelte stehen für das Fehlen von Risiken.

---

<sup>126</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 9.4]



**Abbildung 2-13: OCTAVE<sup>SM</sup> Risikoprofil**

Quelle: Alberts & Dorofee 2002, Abschnitt 9.4

Die OCTAVE<sup>SM</sup>-Methode der Risikoanalyse ist, wie bereits erwähnt, nicht auf Wahrscheinlichkeiten basiert. Dennoch gibt es aufgrund hoher Nachfrage einen Leitfaden, um die Wahrscheinlichkeit in die Methode einzubeziehen. Diese Methode wird an dieser Stelle nicht behandelt, da sie mit der eigentlichen OCTAVE<sup>SM</sup>-Methode zur IT-Sicherheits-Überprüfung nichts zu tun hat. Jedoch ist es wichtig anzumerken, dass die Möglichkeit zur Einbeziehung von Wahrscheinlichkeiten in die OCTAVE<sup>SM</sup>-Methode besteht.<sup>127</sup>

### ***Process 8: Develop Protection Strategy – Workshop A<sup>128</sup>***

Der abschließende Prozess in der OCTAVE<sup>SM</sup>-Methode besteht aus zwei Workshops. Der erste hat die Erstellung einer Schutzstrategie für die Organisation zum Ziel, der zweite die Bestätigung dieser Schutzstrategie durch das obere Management.

Vor dem ersten Workshop werden die gesammelten Informationen aus den Prozessen 1 bis 3 zusammengefasst, falls das nicht schon zuvor gemacht wurde. Die Ergebnisse der Fragebögen werden prozentuell nach den verschiedenen Organisationsebenen berechnet. Aus diesen

<sup>127</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 9.5]

<sup>128</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.1]

Zahlen lässt sich ersehen, ob eine Sicherheitspraxis in der Organisation angewendet wird, nicht angewendet wird, oder ob Unklarheit darüber herrscht. Nicht angewandte oder unklare Sicherheitsmaßnahmen sind Anzeichen für Sicherheitsschwächen. Nach der Auswertung der Fragebögen werden die in den geführten Diskussionen der Prozesse 1 bis 3 gesammelten Informationen zusammengefasst.<sup>129</sup> Nach der Wiederholung und Zusammenfassung dieser Informationen kann der erste Workshop beginnen. Folgende Aktivitäten finden in Workshop 8A statt:

- Wiederholung der Risiko-Informationen
- Erstellung einer Schutzstrategie
- Erstellung von Risikolinderungsplänen
- Erstellung einer Aktionsliste

### *Wiederholung der Risiko-Informationen<sup>130</sup>*

Die Wiederholung der gesammelten Informationen ist nötig, da die OCTAVE<sup>SM</sup>-Methode einen längeren Zeitraum beansprucht, und deshalb wichtige Workshops zu diesem Zeitpunkt einige Zeit zurückliegen. Man beginnt dabei mit den Informationen die zu Beginn des Prozesses 8 wiederholt und zusammengefasst wurden. Dabei muss man beachten, sowohl mit einer globalen als auch mit einer auf Unternehmenswerte gerichteten Perspektive zu arbeiten. Folgende Informationen müssen für jeden kritischen Unternehmenswert wiederholt werden:

- Bedrohungen auf die kritischen Unternehmenswerte
- Areas of Concern der kritischen Unternehmenswerte
- Möglicher Impact auf die Organisation für jede Bedrohung, sowie zugeordnete Bewertungskriterien
- Technologische Schwachstellen der ausgewählten Komponenten
- Empfohlene Maßnahmen, die aus der Schwachstellenanalyse stammen

### *Erstellung einer Schutzstrategie<sup>131</sup>*

In dieser Aktivität wird eine Schutzstrategie für die Organisation erarbeitet. Sie beschreibt, wie die Organisation IT-Sicherheit vorbereitet, implementiert und erhält. Darin sind auch langfristige organisationsweite Aktionen enthalten. Dabei müssen die strategischen und ope-

---

<sup>129</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.2]

<sup>130</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.3]

<sup>131</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.4]

rationalen Praxisbereiche der IT-Sicherheit abgedeckt werden. Die strategischen Praxisbereiche sind:

- IT-Sicherheitsbewusstsein und Training
- IT-Sicherheitsstrategie
- IT-Sicherheitsmanagement
- IT-Sicherheitspolitik und –vorschriften
- IT-Sicherheitsmanagement bei der Arbeit mit externen Organisationen
- Eventualitätenplanung und Disaster Recovery

Die operationalen Praxisbereiche sind:

- Physikalische IT-Sicherheit
- Technologische IT-Sicherheit
- Personalsicherheit

Die Umsetzung der Pläne in allen Bereichen ist im Normalfall nicht gleichzeitig möglich, weshalb wiederum Prioritäten für deren Umsetzung gesetzt werden müssen.

Die Erstellung der Schutzstrategie besteht aus zwei Schritten. Zuerst wird untersucht, welche Maßnahmen den Sicherheitsstandard in den strategischen Praxisbereichen erhalten bzw. verbessern können. Danach wird geprüft, welche Maßnahmen nötig sind, um die Sicherheit in den operationalen Praxisbereichen zu gewährleisten.

Anhand der Interviews und Fragebögen sollte es möglich sein, zu entscheiden, welche derzeit eingesetzten IT-Sicherheitsmaßnahmen weiter verwendet, verbessert, bzw. welche neu eingeführt werden sollten. Die OCTAVE<sup>SM</sup>-Methode liefert Fragestellungen, anhand derer die Erstellung der Schutzstrategien für die Praxisbereiche vereinfacht wird. Die Empfehlungen aus der Schwachstellenanalyse helfen ebenfalls bei der Erstellung der Schutzstrategie für die operationalen Praxisbereiche.

### *Erstellung von Risikolinderungsplänen<sup>132</sup>*

Nach der Erstellung einer Sicherheitsstrategie werden taktische Maßnahmen ausgewählt, um festgestellte Risiken abzuschwächen. Die Perspektive verschiebt sich von der Organisation auf die kritischen Unternehmenswerte. Gegenmaßnahmen werden überlegt, die entweder die

---

<sup>132</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.5]

Impacts abschwächen, oder die zugrunde liegenden Bedrohungen abschwächen. Diese Gegenmaßnahmen bilden die Risikolinderungspläne. Für jeden kritischen Unternehmenswert wird ein solcher Plan erstellt und nach den vier Bedrohungskategorien (menschliche Akteure über Netzwerkzugriff, menschliche Akteure über physikalischen Zugriff, Systemprobleme, andere Probleme) strukturiert. Die Erstellung der Risikolinderungspläne geschieht in vier Schritten.

Der erste Schritt ist die Auswahl des Risikolinderungsansatzes. Hier muss entschieden werden, welche Risiken man akzeptiert und welche gelindert werden sollen. Die Schwere der Impacts ist hier eine Entscheidungshilfe. Beispielsweise kann entschieden werden, alle Impacts, welche als hoch oder mittel (high bzw. medium) eingestuft wurden, zu lindern, die niedrigen (low) Impacts hingegen zu akzeptieren. Die Entscheidung obliegt wiederum dem Analyseteam gemäß dem OCTAVE<sup>SM</sup> Principle der Self-direction. Die Entscheidungen müssen im Risikoprofil des jeweiligen kritischen Unternehmenswerts dokumentiert werden.

Als zweiter Schritt folgt die Auswahl der Risikolinderungs- bzw. Gegenmaßnahmen für jede Bedrohungskategorie jedes kritischen Unternehmenswertes. Die Maßnahmen betreffen die Erkennung einer entstehenden Bedrohung, die Prävention einer Bedrohung, die Wiederherstellung des Systems nach einer Bedrohung, andere Aktionen um das Risiko der Bedrohung zu lindern, sowie die Überprüfung, ob die Maßnahme effektiv funktioniert. Die ausgewählten Maßnahmen können administrativ, physikalisch oder technisch sein. Den Risikolinderungsmaßnahmen werden danach Prioritäten gemäß ihren Kosten und Nutzen, sowie den organisatorischen Einschränkungen bezüglich Personal und Zeitmanagement zugeteilt. Bei der Auswahl der Risikolinderungsmaßnahmen sind eventuelle schnell umsetzbare Aktionen aufzuzeichnen, da diese in der nächsten Aktivität behandelt werden.

Drittens folgt die Suche nach Lücken und Themen in den Risikolinderungsplänen. Die Einzelnen Pläne müssen miteinander konsistent sein. Risikolinderungsmaßnahmen, welche mehr als ein Risiko lindern können, sollten nun mit einer höheren Priorität versehen werden, um ihre Umsetzung zu beschleunigen.

Der vierte Schritt beinhaltet die Überprüfung der im dritten Schritt gefundenen Themen. Es könnte nötig sein, diese Themen in die Schutzstrategie einzuarbeiten. Diese wird hier dementsprechend aktualisiert.

*Erstellung einer Aktionsliste<sup>133</sup>*

Die Aktionsliste bezeichnet Aktionen, die das Personal einer Organisation unmittelbar nach der IT-Sicherheits-Überprüfung ohne Veränderungen der IT-Sicherheitspolitik, Training oder ähnliche Maßnahmen durchführen kann. Beispiele sind das Beauftragen eines Mitarbeiters, die in Prozess 6 entdeckten schwerwiegenden Schwachstellen zu beheben, oder der Auftrag an das Analyseteam, Details zur Aktivierung der Schutzstrategie auszuarbeiten. Die Aktionsliste beinhaltet die durchzuführenden Aktionen, die dafür verantwortlichen Personen, einen Termin zur Fertigstellung der Aktionen, und die notwendigen Unterstützungsmaßnahmen durch das Management.

Abschließend muss erwähnt werden, dass die vorgestellte Reihenfolge der Aktivitäten in Prozess 8A nicht verpflichtend ist. Für manche Organisationen bzw. Analyseteams wird eine andere Reihenfolge natürlicher erscheinen. Dies ist aufgrund der iterativen Struktur der Aktivitäten kein Problem.

***Process 8: Develop Protection Strategy – Workshop B<sup>134</sup>***

Der zweite Teil von Prozess 8 dient dazu, die Sichtweise des oberen Managements in die Schutzstrategie, die Risikolinderungspläne und die Aktionsliste einzuarbeiten. Er ist ein geführter Workshop, an dem das obere Management teilnimmt. Folgende Aktivitäten sind für Prozess 8B nötig:

- Vor dem Workshop: Vorbereitung auf das Treffen mit dem oberen Management
- Präsentation der Risikoinformationen
- Präsentation und Überarbeitung der Schutzstrategie, Risikolinderungspläne und der Aktionsliste
- Erstellung der nächsten Schritte

*Vorbereitung auf das Treffen mit dem oberen Management<sup>135</sup>*

Es ist wichtig, sich auf das Treffen mit dem oberen Management gründlich vorzubereiten, da dessen Repräsentanten meist wenig Zeit zur Verfügung haben. Innerhalb kurzer Zeit müssen die Teilnehmer des folgenden Workshops über die Situation aufgeklärt werden, um deren Input zu erhalten. Es muss verständlich gemacht werden, welche Unternehmenswerte kritisch

---

<sup>133</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 10.6]

<sup>134</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 11.1]

für die Organisation sind, und welche Bedrohungen auf diese einwirken. Das obere Management muss ebenfalls darüber aufgeklärt werden, welche Schutzmaßnahmen derzeit ergriffen werden, und wo Defizite herrschen. Anschließend müssen die ausgearbeiteten Strategien und Pläne zum Schutz der kritischen Unternehmenswerte präsentiert werden.

### *Präsentation der Risikoinformationen<sup>136</sup>*

In dieser Aktivität werden dem oberen Management Hintergrundinformationen präsentiert. Das Ziel ist, dem oberen Management das Verständnis der Schutzstrategie, der Risikolinderungspläne und der Aktionsliste zu ermöglichen. Verwendete Begriffe, die unklar sein können, sollten an dieser Stelle erklärt werden. Darüber hinaus ist es oft sinnvoll, die OCTAVE<sup>SM</sup>-Methode für die Teilnehmer des Workshops zusammenzufassen.

Ein guter Ansatz ist, die Aufmerksamkeit der Teilnehmer auf die kritischen Unternehmenswerte und den Grund für diese Einschätzung zu lenken. Die Ergebnisse der Fragebögen werden präsentiert, gefolgt von den nach Praxisbereichen geordneten Maßnahmen der Schutzstrategie und den organisatorischen Schwachstellen. Zu guter Letzt folgt die Präsentation der Bedrohungs-, Risiko- und Schwachstelleninformation jedes kritischen Unternehmenswertes.

### *Präsentation und Überarbeitung der Schutzstrategie, Risikolinderungspläne und der Aktionsliste<sup>137</sup>*

Nachdem das obere Management ein Verständnis für das Risiko erlangt hat, werden die Schutzstrategie, die Risikolinderungspläne und die Aktionsliste präsentiert. Dabei wird dem oberen Management gezeigt, was diese Begriffe bedeuten. An die Präsentation anschließend werden die Mitglieder des oberen Managements ihre organisationsweite Perspektive einbringen und möglicherweise Veränderungen an den vorgeschlagenen Maßnahmen vorschlagen bzw. verlangen. Die Aufgabe des Analyseteams ist es, das obere Management auf die Folgen der jeweiligen Veränderungen hinzuweisen.

---

<sup>135</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 11.2]

<sup>136</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 11.3]

<sup>137</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 11.4]

### *Erstellung der nächsten Schritte*<sup>138</sup>

Diese Aktivität ist die letzte der IT-Sicherheits-Überprüfung nach der OCTAVE<sup>SM</sup>-Methode. Das obere Management muss nun entscheiden, wie die Ergebnisse implementiert werden sollen. Dies ist der wichtigste Schritt der ganzen IT-Sicherheits-Überprüfung, da hier entschieden wird, wie sich die IT-Sicherheit in der Zukunft entwickeln wird. Das obere Management muss folgende Fragen beantworten:

- Was wird die Organisation tun, um auf die Ergebnisse der IT-Sicherheits-Überprüfung aufzubauen?
- Was wird das obere Management tun, um eine Verbesserung der IT-Sicherheit zu gewährleisten?
- Was wird das obere Management tun, um den Prozess der Verbesserung zu unterstützen? Was können die anderen Managementebenen tun?
- Wie lauten die Pläne für nachfolgende IT-Sicherheits-Überprüfungen?

Nach dem zweiten Workshop von Prozess 8 ist die IT-Sicherheits-Überprüfung abgeschlossen. Die Dokumentation der Ergebnisse ist der letzte Schritt. Das Management sollte dazu angehalten werden, die Ergebnisse nach dem OCTAVE<sup>SM</sup> Principle der Open Communication organisationsweit bekannt zu machen. Die Implementierung der Schutzstrategie, Risikolinderungspläne und Aktionslisten ist die erste Folgeaktivität. Die OCTAVE<sup>SM</sup>-Methode ist hiermit allerdings abgeschlossen.

### ***Outputs der Phase 3***

Folgende Outputs sind das Ergebnis der Phase 3 der OCTAVE<sup>SM</sup>-Methode:<sup>139</sup>

- Risks to Critical Assets: Risiken für kritische Unternehmenswerte
- Risk Measures: Maß für das Risiko; in der OCTAVE<sup>SM</sup>-Methode Risikobewertungskriterien oder optional die Wahrscheinlichkeit eines Impacts
- Protection Strategy: Schutzstrategie
- Risk Mitigation Plans: Risikolinderungspläne

---

<sup>138</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 11.5]

<sup>139</sup> [Vgl. Alberts & Dorofee 2001, S. 39]

### 2.2.3 Variationen des OCTAVE<sup>SM</sup>-Ansatzes<sup>140</sup>

Der OCTAVE<sup>SM</sup>-Ansatz wird durch das Set von Principles, Attributes und Outputs beschrieben. Die OCTAVE<sup>SM</sup>-Methode ist eine Methode zur IT-Sicherheits-Überprüfung, welche mit den OCTAVE<sup>SM</sup>-Kriterien konform geht. Es ist jedoch nicht die einzige vorstellbare Methode, welche die OCTAVE<sup>SM</sup>-Kriterien erfüllt. Es ist vielmehr möglich, die Methode auf verschiedenste Organisationsformen und –umgebungen anzupassen.

#### Mögliche Anpassungen von OCTAVE<sup>SM</sup><sup>141</sup>

Ein Beispiel einer Anpassung ist die Veränderung des Catalog of Practices, um die nötigen Industriestandards einer Domäne (z.B. Finanzmarkt) einzuhalten. Auch die Anpassung des generischen Bedrohungsprofils an die Gegebenheiten ist denkbar.

Eine Organisation, welche geographisch verteilt agiert, kann die OCTAVE<sup>SM</sup>-Methode auf ihre Struktur anpassen. Regierungen haben die Möglichkeit, eine eigene Version der OCTAVE<sup>SM</sup>-Methode zu entwickeln und für Behörden verpflichtend zu machen, um eine Basis für die Kommunikation von IT-Sicherheitsfragen zu schaffen. Durch die Definition der OCTAVE<sup>SM</sup> Principles ist es möglich, auf jede Organisationsumgebung zu reagieren und eine passende Methode zu entwickeln. Wichtig dabei ist nur, den Principles, Attributes und Outputs treu zu bleiben.

Eine weitere mögliche Anpassung ist die Zusammenfassung der Prozesse. Beispielsweise können die Prozesse 1 bis 3 bei kleinen Organisationen mit wenigen Mitarbeitern in einen Prozess zusammengefasst werden.

Darüber hinaus kann eine OCTAVE<sup>SM</sup>-Methode entwickelt werden, welche von organisation fremden Beratern durchgeführt werden. Dafür sind jedoch immer noch organisationseigene Mitarbeiter notwendig, um an den Workshops teilzunehmen. Die Berater übernehmen lediglich die Führung der Prozesse.

Die hier angeführten Anpassungen der OCTAVE<sup>SM</sup>-Methode sind nur eine Auswahl der Möglichkeiten. Wenn man sich an die OCTAVE<sup>SM</sup> Principles, Attributes und Outputs hält, sind vielgestaltige Methoden möglich, welche konsistent mit dem OCTAVE<sup>SM</sup>-Ansatz sind.

---

<sup>140</sup> [Vgl. Alberts & Dorofee 2002, Kap. 12]

<sup>141</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 12.1]

Eine durch CERT/CC entwickelte Variation der OCTAVE<sup>SM</sup>-Methode ist die OCTAVE<sup>SM</sup>-S-Methode. Sie ist auf Organisationen mit bis zu hundert Mitarbeitern ausgelegt, und wird mit Arbeitsmaterial und Implementierungsanleitungen unterstützt.

### **Anpassung der OCTAVE<sup>SM</sup>-Methode an die Organisation<sup>142</sup>**

Grundsätzlich gibt es zwei Arten, die OCTAVE<sup>SM</sup>-Methode an eine Organisation anzupassen:

1. Anpassung der IT-Sicherheits-Überprüfung
2. Anpassung der Arbeitsmittel

### ***Anpassung der IT-Sicherheits-Überprüfung<sup>143</sup>***

Der Ablauf der IT-Sicherheits-Überprüfung kann in einigen Punkten verändert werden, welche in der Folge kurz beschrieben werden.

#### *Reihenfolge der Prozesse*

Vor allem die Reihenfolge der ersten drei Prozesse kann verändert werden, um beispielsweise bei streng hierarchischen Organisationen erst das Personal und danach das Management zu interviewen. Dabei muss jedoch beachtet werden, dass auch das Management ihre Perspektive einbringt, anstatt nur die Ergebnisse der vorherigen Interviews zu kommentieren.

#### *Sichtung der IT-Sicherheitspolitiken*

Die IT-Sicherheitspolitiken können zu Beginn der IT-Sicherheits-Überprüfung sehr sinnvoll sein. So entdeckt man die gültigen Richtlinien und Standards, welche die Organisation erfüllen muss. Die Ergebnisse dieser Sichtung können auch zur Anpassung der IT-Sicherheits-Überprüfung genutzt werden, beispielsweise zur Anpassung des Catalog of Practices.

#### *Zeitplan*

Die Durchführung der OCTAVE<sup>SM</sup>-Methode kann je nach Analyseteam und den anderen Pflichten der Mitglieder zwischen sechs Wochen und sechs Monaten dauern. Kaum eine Organisation kann es sich leisten, ein Analyseteam vollzeitlich für die Durchführung der OCTAVE<sup>SM</sup>-Methode zu beschäftigen. Es sollte jedoch beachtet werden, dass die Durchführung nicht so lange dauert, dass die Ergebnisse veraltet sind, bevor die OCTAVE<sup>SM</sup>-Methode be-

---

<sup>142</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 12.2]

<sup>143</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 12.2.1]

endet wurde. Falls der Zeitplan dennoch stark gestreckt wurde, sollten dringende Aktionen schon vor der Beendigung der OCTAVE<sup>SM</sup>-Methode durchgeführt werden.

### *Anzahl und Form der Workshops*

Die Anzahl der Workshops der Prozesse 1 bis 3 ist flexibel. Je nach Größe der Organisation können mehr oder weniger Workshops nötig sein. Darüber hinaus können einige Workshops kombiniert werden, um Zeit zu sparen (z.B. Workshop 7 und 8A). Wichtig sind die Resultate der Workshops, nicht deren Anzahl. Auch in der Form der Workshops ist Flexibilität gegeben, solange beachtet wird, nur die besten Ergebnisse für die Organisation zu erreichen.

### *Physikalische Sicherheitschwachstellen*

Die Überprüfung der IT-Infrastruktur auf Schwachstellen in Phase 2 kann um einige Aspekte erweitert werden. Die Zugangsrouten ins Gebäude sowie zu Räumen, in denen kritische Dokumente oder IT-Systeme gelagert werden, kann überprüft werden. Darüber hinaus können etwa die Türschlösser und Identifikationsmechanismen auf ihre Sicherheit geprüft werden.

### *Outsourcing*

Outsourcing stellt bei der OCTAVE<sup>SM</sup>-Methode ein Problem dar. Eines der OCTAVE<sup>SM</sup> Principles ist das der Self-direction, welches besagt, dass die IT-Sicherheitsüberprüfung durch organisationseigenes Personal durchgeführt werden soll. Dies ist heutzutage durch verstärktes Outsourcing der IT-Infrastruktur schwierig geworden. Deshalb muss die OCTAVE<sup>SM</sup>-Methode oft auf diese Umgebung angepasst werden. Der Service-Provider der Organisation muss mit der Organisation zusammenarbeiten, um sicherzustellen, dass die IT-Sicherheit gewährleistet ist. Dies wird meist durch Verträge geregelt.

### *Risikowahrscheinlichkeit*

Wie bereits erwähnt (s. Abschnitt 2.2.2), ist es möglich, Risikowahrscheinlichkeiten in den Risikobewertungsprozess einzubinden. Diese Möglichkeit ist mit Vorsicht zu genießen, da eventuell Risiken mit geringer Wahrscheinlichkeit ignoriert werden, jedoch einen katastrophalen Impact nach sich ziehen können.

### *Multiple Impactbewertungen*

In Prozess 7 der OCTAVE<sup>SM</sup>-Methode werden den Impacts Risikobewertungskriterien zugeordnet. Es ist hierbei möglich, jedem der Impactbereiche (Image/Kundenvertrauen, Sicherheit und Gesundheit, Bußgelder und gerichtliche Strafen, Finanzen, Produktivität) eine eigene Impactbewertung zuzuordnen. Dadurch wird es möglich, Risikolinderungspläne gezielt auf bestimmte Impactbereiche abzustimmen, falls beispielsweise Image für eine Organisation wichtiger ist als alle andern Bereiche.

### *Automatisierte Werkzeuge*

Die Verwendung von automatisierten Werkzeugen kann die Datensammlung und –verwaltung während der Durchführung der OCTAVE<sup>SM</sup>-Methode erleichtern. Dazu zählen Datenbanken und Analysewerkzeuge.

### *Unabhängiges internes Analyseteam*

Ein unabhängiges internes Analyseteam kann in einer geographisch verteilten Organisation von Geschäftsstelle zu Geschäftsstelle bzw. Abteilung zu Abteilung reisen, um die OCTAVE<sup>SM</sup>-Methode durchzuführen. Dabei übernimmt das Analyseteam die Aufgabe der Führung der OCTAVE<sup>SM</sup>-Methode, bindet aber das lokale Personal mit ein, um das Principle der Self-direction nicht zu verletzen. Darüber hinaus hilft es bei der Implementierung der Ergebnisse.

### ***Anpassung der Arbeitsmittel<sup>144</sup>***

Selbstverständlich können auch die verschiedenen Arbeitsmittel, welche meist Teil der Veröffentlichungen der OCTAVE<sup>SM</sup>-Methode sind, an unterschiedliche Anforderungen angepasst werden.

### *Catalog of Practices*

Der Catalog of Practices kann an gewissen Standards angepasst werden, welche in bestimmten Domänen üblich sind. Anders können gewisse Sicherheitsmaßnahmen entfernt werden. Das Ziel ist, einen Catalog of Practices zu haben, der für die Organisation sinnvoll und hilfreich ist. An ihm werden die derzeitigen Sicherheitsmaßnahmen während der OCTAVE<sup>SM</sup>-Methode gemessen.

### *Generisches Bedrohungsprofil*

Vor dem Beginn der Durchführung der OCTAVE<sup>SM</sup>-Methode kann das generische Bedrohungsprofil auf die Bedürfnisse der Organisation angepasst werden. Dies ist auf mehrere Arten möglich:

- Hinzufügen einer neuen Bedrohungskategorie
- Hinzufügen neuer Bedrohungen zu einer bestehenden Bedrohungskategorie
- Entfernen von nicht anwendbaren Risiken aus einer Bedrohungskategorie
- Vertiefen einer Bedrohungskategorie

Beispielsweise können die Bedrohungsakteure angepasst werden. Das könnte die Erweiterung der menschlichen Akteure über Netzwerkzugriff auf verschiedene Typen (z.B. Spione, Terroristen, Konkurrenten, Vandalen, Kriminelle, etc.) bedeuten.

Auch die Bedrohungsprofile der kritischen Unternehmenswerte können auf vielfältige Weise angepasst werden. Detailliertere Zugriffspfade oder die Erstellung von separaten Bedrohungsbaumen für unterschiedliche Arten von Netzwerk- oder physikalischem Zugriff sind nur Beispiele für die Möglichkeiten.

Für die meisten Organisationen sind die vorgeschlagenen Bedrohungsprofile jedoch ausreichend. Durch das Hinzufügen von mehr Details wird auch die Analysetätigkeit komplizierter. Dies sollte bei einer Anpassung nicht außer Acht gelassen werden.

### *Worksheets*

Einige Dokumente sind für die Verwendung bei der OCTAVE<sup>SM</sup>-Methode vorgeschlagen. Darunter sind Interviewschemata für die Prozesse 1 bis 3, Bedrohungsprofile, Profile der kritischen Unternehmenswerte, und andere. All diese können frei angepasst werden.

#### **2.2.4 Laufende Entwicklungen von OCTAVE<sup>SM</sup>**

Die laufenden Entwicklungen beschränken sich größtenteils auf die OCTAVE<sup>SM</sup>-S-Methode, welche auf kleine Organisationen zugeschnitten ist und in der Version 0.9 vorliegt. Bisher sind einige Benutzerhilfen noch nicht fertig gestellt, dies wird jedoch für weitere Veröffentli-

---

<sup>144</sup> [Vgl. Alberts & Dorofee 2002, Abschnitt 12.2.2]

chungen angekündigt. Darüber hinaus ist die OCTAVE<sup>SM</sup>-Methode als in ihrer Entwicklung komplett anzusehen.<sup>145</sup>

Zu erwähnen ist noch, dass eine Vielzahl von OCTAVE<sup>SM</sup>-konformen Methoden in Entwicklung stehen kann, da die Entwicklung einer solchen Methode jedem Unternehmen offen steht.<sup>146</sup>

### 2.3 Control Objectives for Information and related Technology - COBIT

COBIT ist ein Framework für IT-Governance und wird vom IT Governance Institute herausgegeben. COBIT erschien erstmals 1996, damals herausgegeben von der ISACF (=Information Systems Audit and Control Foundation). Die zweite Edition, welche 1998 erschien, erfuhr eine Erweiterung der Quelldokumente und der Kontrollziele (Control Objectives), sowie die Veröffentlichung des COBIT Implementation Toolsets. Die dritte und aktuellste Edition von COBIT erschien im Jahr 2000, nun herausgegeben vom IT Governance Institute.<sup>147</sup>

Das IT Governance Institute wurde von der ISACA (=Information Systems Audit and Control Association) 1998 gegründet, um die Anwendung und das Verständnis der Prinzipien der IT-Governance zu unterstützen.<sup>148</sup>

COBIT basiert auf den von der ISACF entwickelten Kontrollziele und wurde durch die Einarbeitung von internationalen technischen, professionellen, regulatorischen und gewerbespezifischen Standards verbessert.<sup>149</sup> COBIT zielt auf die Anwendung auf organisationsweite Informationssysteme ab.

COBIT besteht aus einer Produktfamilie, die hierarchisch aufgebaut ist. Für jeden Teilnehmer an der Implementierung und Aufrechterhaltung eines COBIT-Prozesses sind andere Informationen relevant. Dem trägt der Aufbau von COBIT Rechnung. Die COBIT Produktfamilie wird in Abbildung 2-14 dargestellt. Sie besteht aus sechs Modulen. An oberster Stelle der Hierarchie steht die Executive Summary, welche sich an das obere Management wendet und einen Überblick über die Methodik gibt. Das Framework definiert die Methodik. Das Imple-

---

<sup>145</sup> [Vgl. CERT@/CC, 2003, 2, OCTAVE@ Methods, <http://www.cert.org/octave/methods.html> ]

<sup>146</sup> [Vgl. CERT@/CC, 2003, 2, OCTAVE-Consistent Methodologies, <http://www.cert.org/octave/derivatives.html> ]

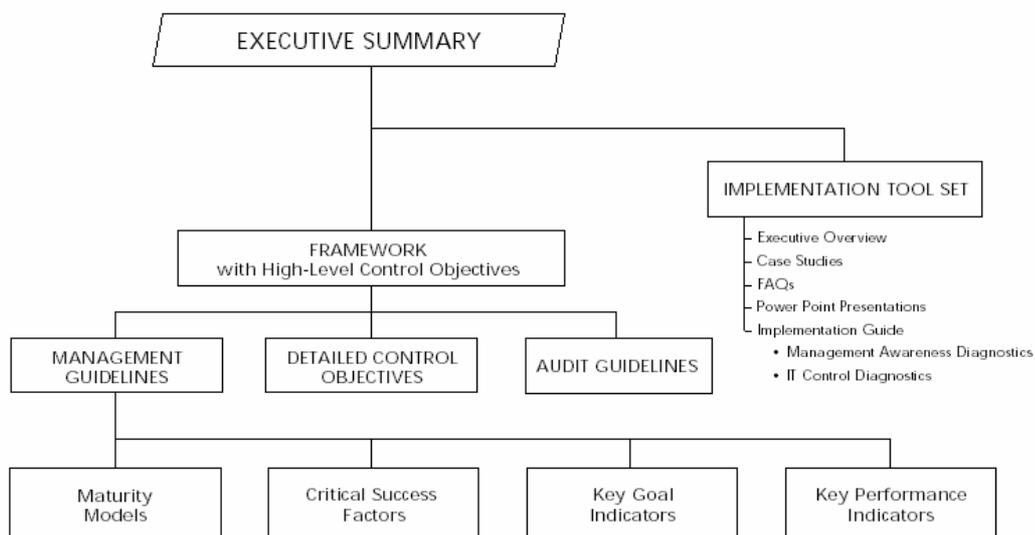
<sup>147</sup> [Vgl. IT Governance Institute, 2000a, S. 11]

<sup>148</sup> [Vgl. IT Governance Institute, 2000a, S. 11]

<sup>149</sup> [Vgl. IT Governance Institute, 2000c, S. 18]

mentation Toolset ermöglicht die Implementierung der Methodik. Die Management Guidelines beschreiben, wie der Erfolg der Methodik gemessen werden kann. Die Control Objectives beschreiben die zu erreichenden Kontrollziele. Die Audit Guidelines beschreiben schließlich, wie man die Methodik auf ihre Funktion überprüft. COBIT ist nur teilweise frei verfügbar. Teile der COBIT Produktfamilie können nur von zahlenden Mitgliedern der ISACA aus dem WWW bezogen werden. Das ganze Paket lässt sich kostenpflichtig in verschiedener Form und zu verschiedenen Preisen bestellen. Zum Download verfügbare Dokumente findet man auf <http://www.isaca.org> bzw. <http://www.isaca.ch>.

## COBIT Family of Products



**Abbildung 2-14: COBIT Produktfamilie**

Quelle: IT Governance Institute, 2000c, S. 19

COBIT ist ein Modell für die IT-Governance. IT-Governance bedeutet, dass die IT Systeme als immer wichtiger werdende Faktoren der Organisation erkannt und in die Organisationsstruktur integriert werden. Viele Organisationen hängen direkt von ihren IT-Systemen ab.

### 2.3.1 COBIT IT-Governance – Die COBIT-Methodik

Fragen, die sich Organisationen, welche IT für ihre Geschäftsprozesse einsetzen, stellen müssen, sind vielfältig. Wie ist es möglich, die IT-Prozesse so zu koordinieren, dass sie den Organisationszielen entsprechen und diese weitestgehend unterstützen? Wie kann man Risiken managen und die Sicherheit der IT-Infrastruktur sicherstellen? Kurz: wie kann man die hete-

rogene und sich schnell ändernde Natur der IT-Systeme in die Organisationspolitik einbeziehen und so den Nutzen maximieren, die Risiken jedoch minimieren?

IT-Governance bietet die Struktur, welche IT-Prozesse, IT-Systeme, und Informationen mit Organisationspolitik und Organisationszielen verbindet. Darüber hinaus beinhaltet die IT-Governance sog. „Best Practices“ für den gesamten Bereich der IT-Performance. Der Vorteil, den der Einsatz eines IT-Governance Ansatzes bringt, ist die Maximierung der Vorteile eines IT-Systems in Bezug auf Wettbewerbsvorteile gegenüber anderen Organisationen.<sup>150</sup>

IT-Governance bedeutet:

- Die IT ist auf die Organisationstätigkeit ausgerichtet, ermöglicht diese und maximiert deren Nutzen
- IT-Ressourcen werden vernünftig und wirtschaftlich eingesetzt
- Das IT-Risikomanagement ist angemessen

IT-Governance ist nicht dasselbe wie IT-Sicherheit. Die IT-Sicherheit ist jedoch Teil der IT-Governance, und untrennbar mit ihr verbunden.

Ein Ansatz für die IT-Governance ist die COBIT-Methodik, beschrieben durch das COBIT Framework und untergeordnete COBIT-Produkte. Das COBIT Framework definiert 34 IT-Prozesse in vier IT-Domänen und einen übergeordneten Kontrollansatz für diese IT-Prozesse. Ergänzt wird das Framework durch die COBIT Control Objectives, welche 318 detaillierte Kontrollziele enthalten, sowie die COBIT Audit Guidelines, um die IT-Prozesse auf ihre Funktion zu überprüfen. Darüber hinaus existieren die COBIT Management Guidelines, welche dem Management ermöglichen, die IT-Prozesse zu kontrollieren und zu messen. Dies wird durch die Definition von Maturity Models, CSFs (=Critical Success Factors), KGIs (=Key Goal Indicators) und KPIs (=Key Performance Indicators) erreicht. Um die COBIT-Methodik zu verstehen, folgt hier die Beschreibung des COBIT Framework.

### **COBIT Framework**

Das COBIT Framework schlägt eine Brücke zwischen den Prinzipien der Enterprise Governance, welche die Abläufe in der Organisation betrifft, und den spezifischeren Modellen für die Kontrolle der IT in der Organisation. Das Ergebnis ist ein Modell der IT-Governance. Ziel ist zunächst, eine IT-Control zu etablieren. *Control* wird definiert als die Summe der Politi-

---

<sup>150</sup> [Vgl. IT Governance Institute, 2000b, S. 5]

ken, Prozeduren, Praktiken und organisatorischen Strukturen, welche so gestaltet sind, dass Organisationsziele erreicht und unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden. Das COBIT zugrunde liegende Konzept ist, dass IT-Control durch die Betrachtung der Information entsteht, welche für die Erreichung der Organisationsziele bzw. Organisationsanforderungen benötigt wird; sowie durch Betrachtung der Informationen als Ergebnis der Anwendung von IT-Ressourcen, welche durch IT-Prozesse gesteuert werden müssen.<sup>151</sup> Abbildung 2-15 verdeutlicht diese Sichtweise.



**Abbildung 2-15: Zyklus der IT-Kontrolle**

Quelle: IT Governance Institute, 2000c, S. 13

### *COBIT Kriterien*

Information muss gewissen Kriterien entsprechen, um die Organisationsziele zu erreichen. Diese werden in COBIT und auch hier in der Folge als „Business Requirements for Information“ bezeichnet. Dazu vereinigt COBIT bekannte Referenzmodelle (Quality Requirements, Fiduciary Requirements, Security Requirements), entfernt Redundanzen, und stellt so eine neue Liste von sieben Business Requirements for Information auf.<sup>152</sup>

1. **Effectiveness** bezeichnet die Notwendigkeit, dass Informationen relevant und den Organisationszielen sachdienlich sind, sowie dass sie rechtzeitig, korrekt, beständig und verwendbar geliefert werden.
2. **Efficiency** bezeichnet die Notwendigkeit, dass die Informationen durch optimalen Einsatz der Ressourcen beschafft werden.
3. **Confidentiality** bezeichnet die Notwendigkeit der Vertraulichkeit von Informationen; d.h. die Sicherheit vor unautorisierter Offenlegung.
4. **Integrity** bezeichnet die Notwendigkeit der Integrität der Informationen, d.h. die Sicherheit vor unautorisierter Veränderung oder Zerstörung, sowie die Richtigkeit in Bezug auf den Geschäftsprozess.
5. **Availability** bezeichnet die Notwendigkeit der Verfügbarkeit der Informationen für den Geschäftsprozess jetzt und in der Zukunft.

<sup>151</sup> [Vgl. IT Governance Institute, 2000c, S. 13]

<sup>152</sup> [Vgl. IT Governance Institute, 2000c, S. 13f]

6. **Compliance** bezeichnet die Notwendigkeit der Übereinstimmung der Informationen mit Gesetzen, Regelungen und Verträgen, denen sich der Geschäftsprozess unterwerfen muss.
7. **Reliability of Information** bezeichnet die Notwendigkeit der Beschaffung von korrekten Informationen, um dem Management Leitung der Organisation und die Erstellung von Reporten zu ermöglichen.

Darüber hinaus benutzt die COBIT-Methodik fünf IT-Ressourcen, welche folgendermaßen definiert sind:<sup>153</sup>

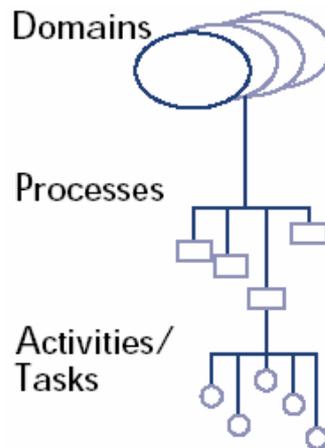
- **Data** sind Daten im weitesten Sinne, strukturiert oder unstrukturiert, Grafiken, Texte, etc.
- **Application Systems** bezeichnet die Summe der manuellen und programmierten Prozeduren.
- **Technology** bezeichnet Hardware, Betriebssysteme, Datenbanksysteme, Netzwerke, Multimedia, etc.
- **Facilities** bezeichnet alle Einrichtungen (Gebäude und Räume), die IT-Systeme beherbergen oder für ihren Support gedacht sind.
- **People** bezeichnet Fähigkeit, Bewusstsein und Produktivität des Personals bei Planung und Organisation, Beschaffung und Implementierung, Betrieb und Unterstützung, und Überwachung der IT-Systeme und IT-Services.

Das COBIT Framework besteht aus übergeordneten Kontrollzielen und einer Gesamtstruktur für ihre Klassifizierung. Die Klassifizierung basiert auf der Betrachtung, dass das Management von IT-Ressourcen auf drei Ebenen passiert. Ganz unten finden die Activities und Tasks statt, welche ein messbares Resultat erzeugen. Der Unterschied zwischen Activities und Tasks ist, dass Activities einem Life Cycle folgen, wohingegen Tasks diskreter Natur sind. Eine Eben darüber befinden sich die Processes. Sie bestehen aus einer Folge von Activities und/oder Tasks. Auf der obersten Ebene werden Processes zu Domains gruppiert. Dieser Aufbau wird in Abbildung 2-16 gezeigt.<sup>154</sup>

---

<sup>153</sup> [Vgl. IT Governance Institute, 2000c, S. 14]

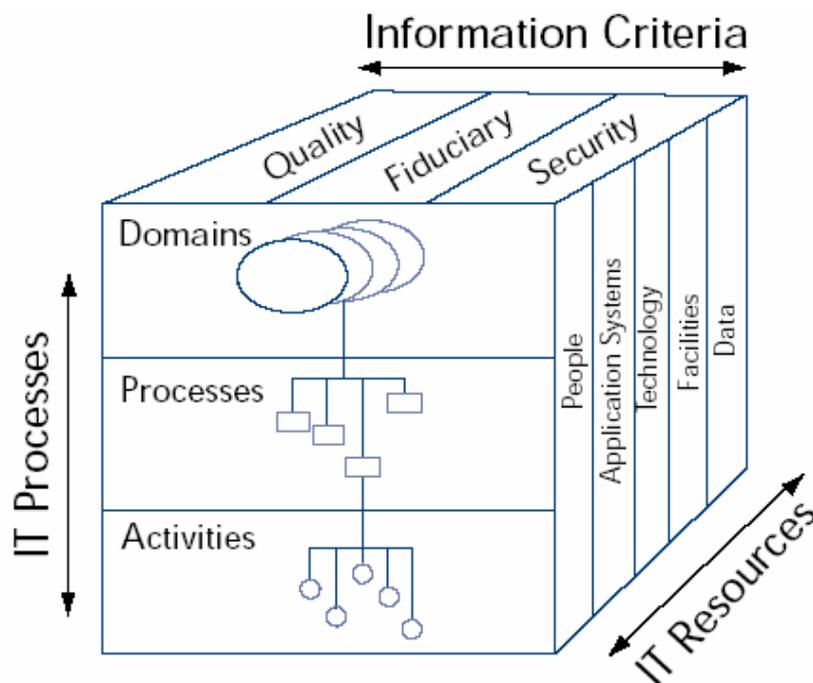
<sup>154</sup> [Vgl. IT Governance Institute, 2000c, S. 16]



**Abbildung 2-16: Die drei Ebenen der IT-Prozesse**

Quelle: IT Governance Institute, 2000c, S. 16

Somit kann das Framework von drei Perspektiven betrachtet werden: Information Criteria (Business Requirements for Information), IT-Ressourcen und IT-Prozesse. Diese Perspektiven werden durch den COBIT Cube (s. Abbildung 2-17) dargestellt.<sup>155</sup>



**Abbildung 2-17: COBIT Cube**

Quelle: IT Governance Institute, 2000b, S. 109

<sup>155</sup> [Vgl. IT Governance Institute, 2000c, S. 16]

### ***COBIT Domänen***

COBIT definiert vier IT-Domänen:

- **Planning and Organisation:** Planung und Organisation
- **Acquisition and Implementing:** Beschaffung und Implementierung
- **Delivery and Support:** Betrieb und Unterstützung
- **Monitoring:** Überwachung

Die Domäne Planning and Organisation beinhaltet Strategien und Taktiken, und die Erkenntnis, wie die IT auf optimale Weise das Erreichen der Organisationsziele unterstützen kann. Darüber hinaus muss die Realisierung der Strategien geplant, kommuniziert und gesteuert werden. Schließlich muss eine angemessene Organisation und technologische Infrastruktur geschaffen werden.<sup>156</sup>

In der Domäne Acquisition und Implementing finden Prozesse statt, welche die gewählte IT-Lösung beschaffen, implementieren, und in die Geschäftsprozesse integrieren. Zusätzlich dazu werden in dieser Domäne Veränderungen und Wartung der IT-Systeme durchgeführt, um den Life Cycle der IT-Systeme fortzuführen.<sup>157</sup>

Delivery and Support bezeichnet jene Domäne, in welcher Prozesse die eigentlichen Dienste zur Verfügung stellen. Diese Dienste sind verschiedenster Natur, von der Datenbearbeitung über IT-Sicherheit bis hin zu Trainings.<sup>158</sup>

In der letzten Domäne, Monitoring, finden schließlich jene Prozesse statt, welche der Überwachung und Qualitätskontrolle der IT-Systeme dienen. Teil dieser Domäne sind die Audits bzw. IT-Control-Überprüfungen.<sup>159</sup>

### ***COBIT Prozesse***

In der COBIT-Methodik werden nun in jeder der vier IT-Domänen IT-Prozesse definiert. Abbildung 2-18 zeigt die in den IT-Domänen stattfindenden IT-Prozesse.

---

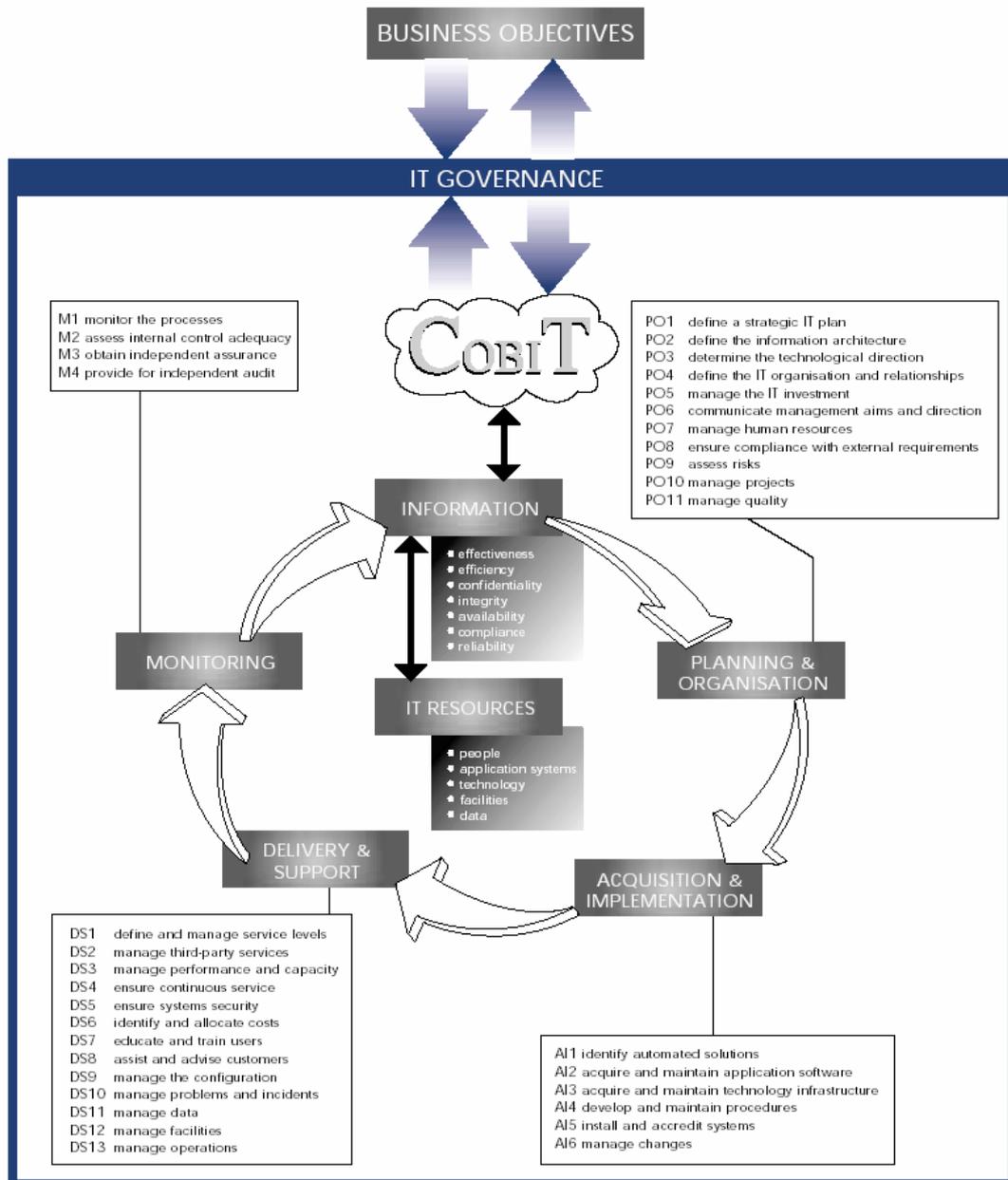
<sup>156</sup> [Vgl. IT Governance Institute, 2000c, S. 16]

<sup>157</sup> [Vgl. IT Governance Institute, 2000c, S. 16]

<sup>158</sup> [Vgl. IT Governance Institute, 2000c, S. 16]

<sup>159</sup> [Vgl. IT Governance Institute, 2000c, S. 16]

## COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



**Abbildung 2-18: COBIT Prozesse in den vier IT-Domänen**

Quelle: IT Governance Institute, 2000c, S. 7

### *COBIT Management Guidelines*

Die COBIT Management Guidelines sind ein Teil der COBIT Produktfamilie. Sie bieten das Werkzeug, um die IT-Prozesse und die dazugehörige IT-Security im Sinne der IT-

Governance zu managen. Dieses Werkzeug sind Indikatoren für die Leistungsmessung der IT-Control und IT-Prozesse, sowie Erfolgsfaktoren, um die Control über die IT-Prozesse zu erreichen.<sup>160</sup> Für jeden der 34 IT-Prozesse sind die jeweiligen Indikatoren im Einzelnen angeführt. Diese Werkzeuge seien an dieser Stelle kurz beschrieben. Für ein Beispiel einer Management Guideline anhand des Prozesses M4 – Provide for Independent Audit siehe Anhang F.

### *Maturity Models*

Die Maturity Models dienen der Bewertung der IT-Control auf einer Skala von 0 bis 5. Das Management kann so für jeden einzelnen der 34 IT-Prozesse eine Note für folgende Aspekte vergeben:<sup>161</sup>

- Enterprise Current Status – Jetziger Status der Organisation
- Industry Best Practice – Vergleichswert: bester Status unter den Mitbewerbern
- International Standard Guidelines – Vergleichswert: Internationale Standards
- Enterprise Strategy – Das Ziel: Unternehmensstrategie für die Zukunft

Die Statusskala der Maturity Models ist folgendermaßen definiert:<sup>162</sup>

0. Non-Existent: Managementprozesse sind nicht vorhanden, die Notwendigkeit dafür wurde noch nicht erkannt.
1. Intitial: Die Prozesse sind unorganisiert und improvisiert, eine Notwendigkeit für die Prozesse wurde jedoch erkannt
2. Repeatable: Die Prozesse folgen einem Plan, werden jedoch ohne Training oder Standardprozeduren durchgeführt; die Verantwortlichkeiten liegen beim Einzelnen, was eine hohe Abhängigkeit und Fehlerwahrscheinlichkeit bedingt
3. Defined: Standardprozeduren wurden entwickelt, dokumentiert, und durch Training kommuniziert. Jedoch liegt die Verantwortung, den Standards zu folgen, beim Einzelnen. Es ist unwahrscheinlich, dass Verletzungen der Standardprozeduren entdeckt werden. Die Prozeduren sind nicht perfektioniert, sondern basieren auf bereits existenten Vorgangsweisen.
4. Managed: Die Überwachung der Prozeduren ist möglich, und Abweichungen bzw. Ineffizienzen werden entdeckt. Prozesse unterliegen einer ständigen Verbesserung. Automation und Werkzeuge werden in eingeschränkter Weise eingesetzt.
5. Optimised: Die Prozesse wurden durch fortlaufende Verbesserungen optimal verfeinert. Automation ist in der IT verbreitet, Werkzeuge verbessern die Effektivität und Qualität, was die Organisation anpassungsfähig macht.

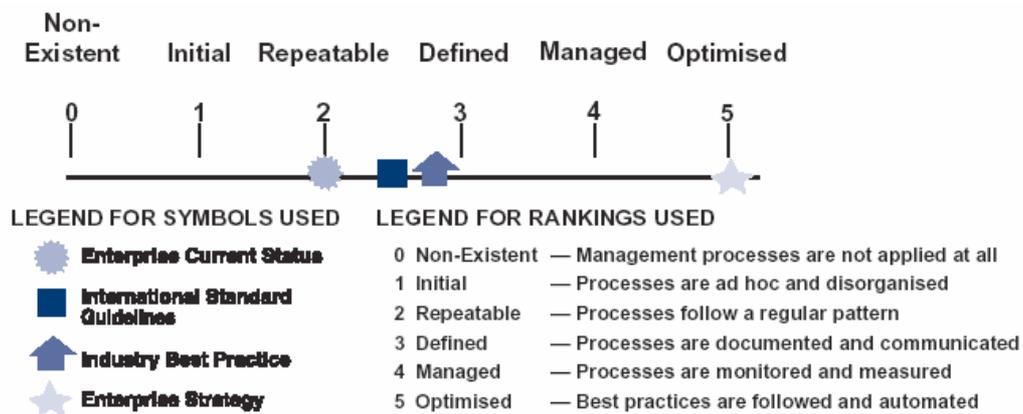
---

<sup>160</sup> [Vgl. IT Governance Institute, 2000b, S. 5]

<sup>161</sup> [Vgl. IT Governance Institute, 2000b, S. 8]

<sup>162</sup> [Vgl. IT Governance Institute, 2000b, S. 11]

Ein Beispiel für ein Maturity Model findet sich in Abbildung 2-19.



**Abbildung 2-19: COBIT Maturity Models**

Quelle: IT Governance Institute, 2000b, S. 8

### *CSFs - Critical Success Factors*

Die CSFs sind jene Aktionen und Maßnahmen, die das Management unternehmen muss, um die IT-Control zu etablieren. Sie sind managementtechnisch orientiert und definieren die wichtigsten strategischen, technischen, organisatorischen und prozedurbezogenen Maßnahmen.<sup>163</sup>

### *KGIs - Key Goal Indicators*<sup>164</sup>

Die KGIs sind Indikatoren für das Management, ob ein IT-Process die Business Requirements of Information erfüllt hat. Meist sind sie als Ziele definiert, die erreicht werden müssen. Normalerweise werden diese Ziele ausgedrückt als:

- Verfügbarkeit der IT-Systeme und IT-Dienste
- Fehlen von Integritäts- und Vertraulichkeitsrisiken
- Kosteneffizienz von IT-Prozessen
- Bestätigung von Verlässlichkeit, Effektivität und Compliance

### *KPIs - Key Performance Indicators*<sup>165</sup>

Die KPIs dienen als Maß dafür, wie gut die Performanz eines IT-Prozesses in Bezug auf die Erreichung der Business Requirements of Information ausfällt. An den KPIs lässt sich able-

<sup>163</sup> [Vgl. IT Governance Institute, 2000b, S. 8]

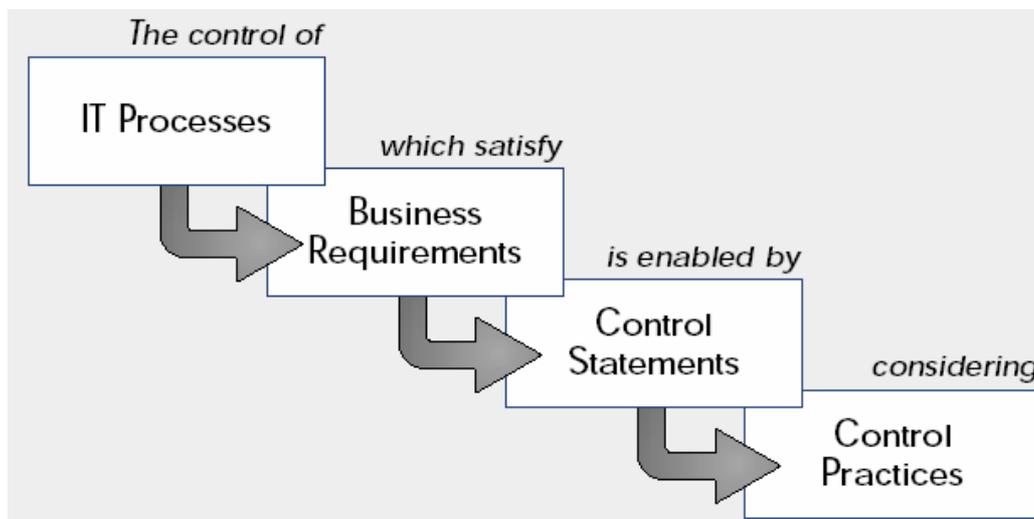
<sup>164</sup> [Vgl. IT Governance Institute, 2000b, S. 8]

<sup>165</sup> [Vgl. IT Governance Institute, 2000b, S. 8]

sen, wie wahrscheinlich die Erreichung eines Zieles ist, und wie gut die eingesetzten Fähigkeiten und Praktiken sind.

### *COBIT Control Objectives*

Die COBIT Control Objectives definieren zusätzlich zu den übergeordnetet Kontrollzielen des COBIT Frameworks noch detaillierte Kontrollziele für jeden einzelnen der 34 IT-Prozesse; insgesamt ergeben sich somit 318 Kontrollziele.<sup>166</sup> Jedes Kontrollziel ist durch eine Gliederung beschrieben, welche in Abbildung 2-20 veranschaulicht wird.



**Abbildung 2-20: Gliederung der Kontrollziele**

Quelle: IT Governance Institute, 2000c, S. 21

Die IT-Control über einen bestimmten Prozess, welche Business Requirements of Information erfüllt, wird durch Control Statements ermöglicht, unter Berücksichtigung von Control Practices. Dieser Aufbau wird am besten durch ein Beispiel erläutert:

*Die Kontrolle über den IT-Prozess DS5 – Ensure System Security,*

*welche die Business Requirements of Information Schutz vor Informationen gegen unautorisierte Benutzung, Offenlegung oder Modifizierung, Schaden oder Verlust*

*erfüllt, wird ermöglicht durch logische Zugangskontrollen, welche sicherstellen, dass Zugriff zu Systemen, Daten und Programmen auf autorisierte Benutzer beschränkt ist*

*unter Berücksichtigung von*

<sup>166</sup> [Vgl. IT Governance Institute, 2000d, S. 21]

- Autorisation, Authentisierung und Zugangskontrollen
- Benutzeridentifikation und Autorisationsprofile
- Benutzertraining
- Usw.

Die Kontrollziele sind so gestaltet, dass eine Navigation nach den drei Flächen des COBIT Cube möglich ist.<sup>167</sup>

### 2.3.2 IT-Sicherheits-Überprüfung in COBIT

Die Überprüfung der IT-Control und damit indirekt der IT-Sicherheit erfolgt durch die Verwendung der COBIT Audit Guidelines. Sie sind ein Werkzeug, um das COBIT Framework und die Control Objectives in einer IT-Control-Überprüfung (=Audit) anzuwenden, und bieten eine einfache Struktur, um die IT-Control zu überprüfen. Da die Audit-Prozeduren von Organisation zu Organisation sehr unterschiedlich sind, und eine Vielzahl von Personal an ihrer Durchführung beteiligt sein kann, sind die COBIT Audit Guidelines sehr allgemein gehalten. Dadurch, dass die COBIT Audit Guidelines auf den COBIT Control Objectives aufbauen, wird die subjektive Meinung des Auditors aus dem Ergebnis entfernt und durch die COBIT zugrunde liegenden Standards ersetzt. Die COBIT Audit Guidelines entfalten ihre volle Wirkung nur, wenn sie in Verbindung mit dem COBIT Framework und den COBIT Control Objectives verwendet werden. Sie sind jedoch nicht für alle Umgebungen gleichermaßen geeignet und können eine Anpassung benötigen. Grundsätzlich versuchen die Audit Guidelines zu beantworten, ob die Organisation die Prozesse korrekt ausführt, und wenn nicht, wie dies korrigiert werden kann. Darüber hinaus können sie auch vorsorglich bei der Prozessentwicklung eingesetzt werden, um Probleme gar nicht erst entstehen zu lassen.<sup>168</sup> Die IT-Sicherheit ist im COBIT Auditprozess nur in dem Maße relevant, wie es IT-Prozesse bezüglich der IT-Sicherheit gibt. Da jedoch die IT-Prozesse alle der Erreichung der Business Requirements of Information verpflichtet sind, und die Business Requirements of Information auch Sicherheitskriterien enthalten, sind IT-Sicherheit und IT-Control direkt miteinander verwoben. Der Aufbau und die Anwendung der Audit Guidelines werden in der Folge beschrieben.

---

<sup>167</sup> [Vgl. IT Governance Institute, 2000c, S. 22]

<sup>168</sup> [Vgl. IT Governance Institute, 2000e, S. 20]

### ***COBIT Audit Guidelines***

Eine IT-Control-Überprüfung hat gemäß den COBIT Audit Guidelines folgende Ziele:<sup>169</sup>

- Lieferung einer vernünftigen Versicherung an das Management, dass die Control Objectives erfüllt werden
- Begründung der durch Control-Schwächen entstehenden Risiken
- Beratung des Managements bezüglich nötiger Korrekturmaßnahmen

Der IT-Prozess wird folgendermaßen überprüft:

1. **Erlangen** von Verständnis über die Geschäftsanforderungen, Organisationsstruktur, Konzepte und Verfahren, Gesetze und Richtlinien, relevante implementierte Kontrollmaßnahmen
2. **Beurteilen** der Angemessenheit und Vorhandensein der angegebenen Verfahren und Kontrollen, Klarheit der Verantwortlichkeiten
3. **Überprüfen** der Compliance durch Tests, ob die angegebenen Kontrollen arbeiten wie gewünscht; konsistent und durchgehend
4. **Aufzeigen** der Risiken, die durch Nichterreichung von Kontrollzielen entstehen; sowie resultierende Bedrohungen und Auswirkungen

Diese Struktur wurde in die COBIT Audit Guidelines eingearbeitet.

Zur Anwendung der Audit Guidelines ist schichtenorientiert, auf die Organisationsziele ausgerichtet, prozessgesteuert, und konzentriert sich auf die IT-Ressourcen und Business Requirements of Information.<sup>170</sup>

Auf der obersten Schicht wird dieser allgemeine IT-Control-Ansatz unterstützt durch:<sup>171</sup>

- Das COBIT Framework, insbesondere die IT-Prozesse, IT-Ressourcen und Business Requirements of Information,
- Voraussetzungen für die IT-Control-Überprüfung (Audit Process Requirements),
- die allgemeinen Audit Guidelines,
- und allgemeine Prinzipien des Control-Prozesses

Die zweite Schicht bilden die detaillierten Audit-Guidelines eines jeden IT-Prozesses. Diese Guidelines werden in einer Standardvorlage geliefert, welche der generellen Struktur „Erlan-

---

<sup>169</sup> [Vgl. IT Governance Institute, 2000e, S. 21]

<sup>170</sup> [Vgl. IT Governance Institute, 2000e, S. 21]

<sup>171</sup> [Vgl. IT Governance Institute, 2000e, S. 21]

gen, Beurteilen, Überprüfen und Aufzeigen“ folgt. Diese Vorlage wurde sowohl auf die allgemeinen als auch auf die detaillierten Audit Guidelines angewandt.<sup>172</sup>

Auf der dritten und letzten Schicht kann der Auditor die Audit Guidelines mit Punkten ergänzen, welche auf lokale Gegebenheiten Rücksicht nehmen. Dies können Industriestandards, plattformspezifische Elemente oder ähnliches sein.<sup>173</sup>

Den Aufbau der drei Schichten ist Abbildung 2-21 zu entnehmen, eine Erläuterung der Elemente folgt direkt danach.

<b>DETAILED STRUCTURE FOR AUDIT GUIDELINES APPLICATION</b>	
<b>Level 1</b> General IT audit approach	<ul style="list-style-type: none"> <li>┆ COBIT <i>Framework</i></li> <li>┆ Audit Process Requirements</li> <li>┆ Control Observations</li> <li>┆ Generic Audit Guideline</li> </ul>
<b>Level 2</b> Process audit guidelines	<ul style="list-style-type: none"> <li>┆ Detailed <i>Audit Guidelines</i></li> </ul>
<b>Level 3</b> Audit attention points to complement detailed control objectives	<ul style="list-style-type: none"> <li>┆ Local Conditions               <ul style="list-style-type: none"> <li>• sector specific criteria</li> <li>• industry standards</li> <li>• platform specific elements</li> <li>• detailed control techniques used</li> </ul> </li> </ul>

**Abbildung 2-21: Schichtenaufbau der COBIT Audit Guidelines**

Quelle: IT Governance Institute, 2000e, S. 22

Das COBIT Framework wurde bereits beschrieben, weswegen die Betrachtung der Elemente der Schicht 1 des Audit-Prozesses mit den Audit Process Requirements beginnt. Zuerst wird bestimmt, welches der angestrebte Horizont der IT-Control-Überprüfung ist. Dazu müssen folgende Informationen gesammelt bzw. definiert werden:<sup>174</sup>

- betroffene Geschäftsprozesse
- IT-Plattformen, IT-Systeme und ihre Verbindungen zueinander
- IT-Verantwortlichkeiten, sowie Daten über Outsourcing und Organisationsstruktur

Danach müssen die Requirements of Information bestimmt werden, die in direktem Zusammenhang mit den Geschäftsprozessen stehen. Anschließend werden die Risiken und der all-

<sup>172</sup> [Vgl. IT Governance Institute, 2000e, S. 21]

<sup>173</sup> [Vgl. IT Governance Institute, 2000e, S. 21]

gemeine Level von Control bestimmt. Auf diesen Informationen aufbauend werden die relevanten IT-Prozesse und damit verbundene IT-Ressourcen bestimmt. Manche Prozesse müssen dadurch mehrmals überprüft werden, jeweils für eine verschiedene IT-Plattform bzw. IT-Ressource. Abschließend sollte eine Audit-Strategie festgelegt werden.<sup>175</sup> Die Audit Process Requirements werden in Abbildung 2-22 dargestellt.

**AUDIT PROCESS REQUIREMENTS**

<ul style="list-style-type: none"> <li>• <b>define audit scope</b></li> </ul>	<ul style="list-style-type: none"> <li>└ business process concerned</li> <li>└ platforms, systems and their interconnectivity, supporting the process</li> <li>└ roles, responsibilities and organisational structure</li> </ul>
<ul style="list-style-type: none"> <li>• <b>identify information requirements relevant for the business process</b></li> </ul>	<ul style="list-style-type: none"> <li>└ relevance to the business process</li> </ul>
<ul style="list-style-type: none"> <li>• <b>identify inherent IT risks and overall level of control</b></li> </ul>	<ul style="list-style-type: none"> <li>└ recent changes and incidents in business and technology environment</li> <li>└ results of audits, self-assessments and certification</li> <li>└ monitoring controls applied by management</li> </ul>
<ul style="list-style-type: none"> <li>• <b>select processes and platforms to audit</b></li> </ul>	<ul style="list-style-type: none"> <li>└ processes</li> <li>└ resources</li> </ul>
<ul style="list-style-type: none"> <li>• <b>set audit strategy</b></li> </ul>	<ul style="list-style-type: none"> <li>└ controls X risk</li> <li>└ steps and tasks</li> <li>└ decision points</li> </ul>

**Abbildung 2-22: COBIT Audit Process Requirements**

Quelle: IT Governance Institute, 2000e, S. 23

Das nächste Element der Schicht 1 sind die allgemeinen Audit Guidelines. Sie werden in Abbildung 2-23 dargestellt. Sie folgen der Struktur „Erlangen, Beurteilen, Überprüfen und Aufzeigen“. Sie sind auf alle IT-Prozesse anwendbar und sind auf das Verständnis des IT-Prozesses und dessen Eigentümer ausgerichtet. Die allgemeinen Audit Guidelines sind Grundlage der detaillierten Audit Guidelines.<sup>176</sup>

<sup>174</sup> [Vgl. IT Governance Institute, 2000e, S. 22]

<sup>175</sup> [Vgl. IT Governance Institute, 2000e, S. 22f]

<sup>176</sup> [Vgl. IT Governance Institute, 2000e, S. 23]

## GENERIC AUDIT GUIDELINE

### OBTAINING AN UNDERSTANDING

*The audit steps to be performed to document the activities underlying the control objectives as well as to identify the stated control measures/procedures in place.*

Interview appropriate management and staff to gain an understanding of:

- Business requirements and associated risks
- Organisation structure
- Roles and responsibilities
- Policies and procedures
- Laws and regulations
- Control measures in place
- Management reporting (status, performance, action items)

Document the process-related IT resources particularly affected by the process under review. Confirm the understanding of the process under review, the Key Performance Indicators (KPI) of the process, the control implications, e.g., by a process walk through.

### EVALUATING THE CONTROLS

*The audit steps to be performed in assessing the effectiveness of control measures in place or the degree to which the control objective is achieved. Basically deciding what, whether and how to test.*

Evaluate the appropriateness of control measures for the process under review by considering identified criteria and industry standard practices, the Critical Success Factors (CSF) of the control measures and applying auditor professional judgment.

- Documented processes exist
- Appropriate deliverables exist
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Conclude the degree to which the control objective is met.

### ASSESSING COMPLIANCE

*The audit steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously and to conclude on the appropriateness of the control environment.*

Obtain direct or indirect evidence for selected items/periods to ensure that the procedures have been complied with for the period under review using both direct and indirect evidence.

Perform a limited review of the adequacy of the process deliverables.

Determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

### SUBSTANTIATING THE RISK

*The audit steps to be performed to substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources. The objective is to support the opinion and to 'shock' management into action. Auditors have to be creative in finding and presenting this often sensitive and confidential information.*

Document the control weaknesses, and resulting threats and vulnerabilities.

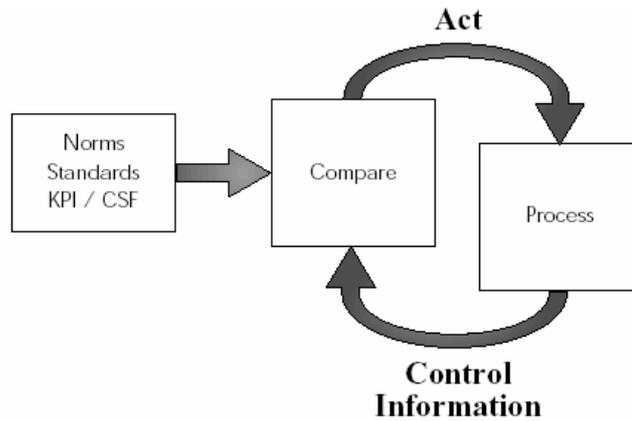
Identify and document the actual and potential impact; e.g., through root-cause analysis.

Provide comparative information, e.g., through benchmarks.

### Abbildung 2-23: COBIT Allgemeine Audit Guidelines

Quelle: IT Governance Institute, 2000e, S. 25

Der Control-Prozess an sich kann auch zur Ergänzung der Audit Guidelines beitragen. Er besteht aus 4 Schritten, und wird in Abbildung 2-24 veranschaulicht.



**Abbildung 2-24: Struktur des Control-Prozesses**

Quelle: IT Governance Institute, 2000e, S. 24

Zuerst wird ein Standard für den IT-Prozess gewählt. Der IT-Prozess liefert Control-Informationen, welche mit den Standards verglichen wird. Aufgrund der Ergebnisse des Vergleiches wird dann agiert, und der IT-Prozess dementsprechend verändert.<sup>177</sup>

Schicht 2 besteht aus den detaillierten Audit Guidelines. Sie sind das Herzstück der COBIT Audit Guidelines. Für jeden IT-Prozess wurde eine detaillierte Audit Guideline ausgearbeitet. Eine detaillierte Audit Guideline beschreibt, durch welche Aktionen man für den betreffenden IT-Prozess der Struktur „Erlangen, Beurteilen, Überprüfen und Aufzeigen“ folgt. Dies beinhaltet, welche Personen zu interviewen sind, welche Informationen gesammelt werden müssen, welche Überlegungen angestellt werden müssen, welche Tests durchgeführt werden müssen, und welche weiteren Aktionen nötig sind. Die detaillierten Audit Guidelines definieren darüber hinaus, welche Ergebnisse die IT-Control-Überprüfung für jeden Prozess haben sollte. Durch Benutzung der detaillierten Audit Guidelines ist es in den meisten Fällen möglich, die IT-Control-Überprüfung erfolgreich durchzuführen; Voraussetzung dafür ist natürlich die Verwendung des COBIT Framework für die IT-Control.

Auf der dritten Schicht erfolgt die Anpassung der IT-Control-Überprüfung auf die Gegebenheiten, die speziell für den Anwendungsbereich gelten, so wie Industriestandards oder plattform-spezifische Eigenschaften.

Zusammenfassend ist zu sagen, dass die detaillierten Audit Guidelines durch die Betrachtung der allgemeinen Audit Guidelines und des überprüften IT-Prozesses ergänzt werden können. Die Erstellung der IT-Control-Überprüfung kann wiederum durch die Audit Process Requi-

<sup>177</sup> [Vgl. IT Governance Institute, 2000e, S. 23]

rements, das COBIT Framework und die übergeordneten Control Objectives profitieren.<sup>178</sup> Anpassungen an lokale Gegebenheiten sind ebenfalls möglich.

### 2.3.3 Laufende Entwicklungen von COBIT

Die COBIT-Methodik wird ebenfalls online angeboten. „COBIT Online“ in der Version 3.2 bietet für registrierte, zahlende Mitglieder die Möglichkeit, alle COBIT Dokumente einzusehen bzw. herunterzuladen. Darüber hinaus stehen Benchmarks für die COBIT-Methodik zur Verfügung. COBIT Online ist im WWW auf der Homepage der ISACA erreichbar, unter <http://www.isaca.org>. COBIT Online wächst durch das Feedback der Anwender und erlaubt den Anwendern die neuesten Elemente noch vor dem nächsten vollständigen Release zu verwenden. Das Feedback der Anwender wird in der Zukunft zu einem neuen Release der COBIT-Methodik – die vierte Edition – führen.

## 2.4 Weitere Standards und Methodiken

Abgesehen von den in der vorliegenden Arbeit detailliert behandelten Methodiken existieren noch eine Vielzahl anderer Standards und Methodiken, welche die IT-Sicherheit betreffen, von unterschiedlichen Institutionen veröffentlicht.

Bevor die Methodiken miteinander verglichen werden, ist es sinnvoll, einen Überblick über die wichtigsten ihnen zugrunde liegenden Normen sowie über weitere Methodiken zu gewinnen.

### ISO/IEC 17799

Die ISO/IEC 17799 ist ein von der ISO herausgegebener Leitfaden für das Management von Informationssicherheit. Die ISO/IEC 17799 ist auch als CoP (=Code of Practice) bekannt. Inhalt sind praxisorientierte Mindestanforderungen im IT-Sicherheitsbereich. Themen sind physische, organisatorische und logische IT-Sicherheit, Anwendungsentwicklung und –unterhalt, Notfallmaßnahmen und –vorsorge, sowie Einhaltung der IT-Sicherheit und IT-Sicherheits-Überprüfungen. Sie folgt einem Grundschutzansatz und setzt zusätzlich durch sog. Key Controls (Schlüsselanforderungen) Schwerpunkte.<sup>179</sup> Die ISO/IEC 17799 dient als Quelle und Referenz für die Entwicklung vieler Methodiken im Bereich der IT-Sicherheit.

---

<sup>178</sup> [Vgl. IT Governance Institute, 2000e, S. 26]

<sup>179</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 5]

## **ISO 9000**

Die ISO 9000 Quality Management Systems definiert Normen für das Qualitätsmanagement, sowie ein Prüfverfahren, mit dem dieses überprüft werden kann. Sie verlangt, dass die IT den Anforderungen gerecht wird.<sup>180</sup>

## **ITSEC/CC**

ITSEC und die CC (=Common Criteria) sind Evaluationskriterien und definieren ein strukturiertes, dokumentiertes Prüfverfahren für IT-Systeme und IT-Produkte. Das Ziel sind nachvollziehbare und vergleichbare Ergebnisse. Dies geschieht durch Definition von funktionalen und qualitativen Anforderungen an die Untersuchungsgegenstände betreffend deren Eigenschaften und deren Entwicklungsverfahren.<sup>181</sup>

Verwendungszweck der ITSEC/CC sind vornehmlich IT-Sicherheits-Überprüfungen und keine Überprüfungen der gesamten IT. Darüber hinaus dienen sie Herstellern von Software und Hardware als Anforderungskatalog an deren Produkte. Die CC bilden einen internationalen Standard: ISO 15408 Evaluation Criteria for IT Security.

## **Marion**

Marion (Méthode d'Analyse des Risques Informatiques et d'Optimisation par Niveau) ist eine Methode zur Beurteilung der IT-Sicherheit. Sie ist kostenpflichtig und vor allem im französischen Raum verbreitet. Eine IT-Sicherheits-Überprüfung unter Verwendung von Marion läuft in drei Phasen ab.<sup>182</sup>

In der ersten Phase werden durch strukturierte Interviews und Risikoszenarien die Risiken, welche die Fortführung der Organisationsprozesse bedrohen, identifiziert. Anschließend werden in der zweiten Phase 27 Bereiche der IT-Sicherheit anhand eines jährlich aktualisierten Fragebogens bewertet und graphisch dargestellt. In der dritten Phase werden aus einer Erfahrungsdatenbank standardisierte Maßnahmen in Form von funktionalen Anforderungen und Implementierungsvorschlägen ausgewählt.<sup>183</sup>

---

<sup>180</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 9]

<sup>181</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 8]

<sup>182</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 19f]

<sup>183</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 5]

## 2.5 Vergleich der Methodiken

Wie nun klar geworden ist, existieren eine Vielzahl an Methodiken und Standards, welche die IT-Sicherheit betreffen. Für eine Organisation stellt sich nun die Frage, welche Methodik die beste ist. So einfach diese Frage klingt, so schwierig ist sie zu beantworten. Aufgrund der unübersichtlichen und sich ständig ändernden Welt der Informationstechnologie ist ein direkter Vergleich zwischen den Methodiken schwierig anzustellen und eine objektive Beantwortung der Frage nach der besten Methodik schlichtweg unmöglich. Darüber hinaus stellen verschiedene Organisationen naturgemäß verschiedene Anforderungen an eine Methodik. Wo ein Unternehmen eine möglichst kosteneffiziente Lösung sucht, wird eine Organisation mit hohen Anforderungen an die IT-Sicherheit – wie etwa eine Bank – eine Methodik bevorzugen, welche einen möglichst hohen und umfassenden Level der IT-Sicherheit erzielt, selbst wenn sie mit erhöhten Kosten verbunden sein sollte.

Die verschiedenen Anforderungen, welche eine Organisation an eine Methodik stellt, können helfen, einen Vergleich der Methodiken durchzuführen. Dies geschieht durch die Erstellung von Vergleichskriterien, welche die möglichen Anforderungen möglichst lückenlos abdecken.

### 2.5.1 Vergleichskriterien

Bei der Erstellung der Vergleichskriterien muss darauf geachtet werden, alle für eine Organisation interessanten Eigenschaften zu integrieren. Der Vergleich der Methodiken geschieht in der vorliegenden Arbeit anhand von zehn Vergleichskriterien, welche in der Folge aufgelistet und beschrieben werden. Die Auswahl der Vergleichskriterien erfolgte anhand von [Initiative D<sup>21</sup>, 2001] und [ISACA Switzerland Chapter, 1998].

#### **Standardisierung**

Standardisierung bezieht sich auf die Verwendung von international abgestützten Methoden und Verfahren und die Verwendung von internationalen Normen und Standards bei der Entwicklung der betreffenden Methodik. Breite internationale Anerkennung fällt ebenso in dieses Kriterium wie die standardisierte Anwendung und Darstellung von Methoden, Verfahren und Resultaten der Methodik.

### **Unabhängigkeit**

Unabhängigkeit bedeutet, dass die Methodik ohne Hilfe Dritter (z.B. Hersteller, Berater) von der Organisation selbst durchführbar ist.

### **Umsetzbarkeit**

Eine gute Umsetzbarkeit bedeutet, dass die Methodik und die Ergebnisse praxis- und maßnahmenbezogen sind, und sich unmittelbar in konkrete Maßnahmen umsetzen lassen.

### **Anpassungsfähigkeit/Skalierbarkeit**

Unter Anpassungsfähigkeit wird die Fähigkeit einer Methodik verstanden, sich an die verschiedensten Organisationsstrukturen und –größen anzupassen. Darüber hinaus bezeichnet dieses Kriterium die Möglichkeit der inhaltlichen Anpassung an spezifische Bedürfnisse der Organisation, etwa durch modularen Aufbau.

### **Einfachheit der Anwendung und Tool-Unterstützung**

Die Einfachheit der Anwendung bedeutet die Möglichkeit, eine Methodik mit geringem Lernaufwand effizient nutzen zu können, sowie eine gewisse Robustheit der Methodik, und die Unterstützung der Arbeitsweise des Anwenders durch die Methodik. Das Vorhandensein von Werkzeugen, welche die Methodik unterstützen, ist ebenfalls Teil dieses Kriteriums.

### **Beurteilungsumfang/Vollständigkeit**

Das Kriterium Beurteilungsumfang/Vollständigkeit verlangt von einer Methodik, dass sie die vollständige Breite des Themenbereiches bearbeitet und in ihrer Bearbeitungstiefe skalierbar ist. Die Betrachtung des Themenbereiches darf sich nicht auf Teilaspekte beschränken.

### **Präsentation der Ergebnisse**

Die Präsentation der Ergebnisse sollte rasch und leicht verständlich in einer gut nutzbaren Form erfolgen.

### **Effizienz**

Effizienz bedeutet, dass die Methodik innerhalb von angemessener Zeit zu Ergebnissen führt, und in ihrem Kosten/Nutzen-Verhältnis ausgeglichen und transparent ist.

### **Aktualität/Updatefrequenz**

Das Kriterium der Aktualität/Updatefrequenz bezieht sich auf die Häufigkeit und Vollständigkeit der Aktualisierungen der Methodik. Auch die Abwärtskompatibilität der Veröffentlichungen ist ein Aspekt der Aktualität.

### **Zertifizierbarkeit**

Zertifizierbarkeit bedeutet, dass die Methodik eine Zertifizierung der Anwender durch Dritte zulässt oder sogar unterstützt.

### **2.5.2 Anwendung der Vergleichskriterien**

Nun wird geprüft, inwieweit die zu vergleichenden Methodiken die Vergleichskriterien erfüllen. Folgende Methodiken nehmen an dem Vergleich teil:

- BSI Grundschatz
- OCTAVE<sup>SM</sup>
- COBIT
- ISO/IEC 17799
- Marion

Die Anwendung der Vergleichskriterien erfolgt an dieser Stelle durch eine Zuordnung der Methodiken an die Vergleichskriterien, und nicht umgekehrt. Dadurch können die Methodiken anhand der Kriterien einfacher verglichen werden.

### **Standardisierung**

#### ***BSI Grundschatz***

Die BSI Grundschatz-Methodik bietet ein hohes Maß an Standardisierung. Als Basis dafür dient die ISO/IEC 17799, die jedoch noch um einige Aspekte erweitert wird. Die BSI Grundschatz-Methodik findet breite Verwendung und ein hohes Maß an internationaler Unterstützung. Selbst auch als Grundlage für die Entwicklung von Sicherheitshandbüchern wie z.B. das Ö-IT-SHB verwendet, ist die BSI Grundschatz-Methodik ein Quasi-Standard im IT-Sicherheits-Bereich. Durch eine Übersetzung ins Englische wird die internationale Anwendung unterstützt. Die Anwendung der Methodik ist standardisiert.

### ***OCTAVE<sup>SM</sup>***

OCTAVE<sup>SM</sup> baut auf verschiedene Internationale Normen auf, darunter die BS 7799, welche der ISO/IEC 17799 entspricht, sowie einem Standard der CERT/CC. Diese Standards fließen in den Catalog of Practices ein.<sup>184</sup> OCTAVE<sup>SM</sup> stützt sich somit auf eine relativ breite Basis international anerkannter Standards. Durch die OCTAVE<sup>SM</sup> Principles, Attributes und Outputs sind die Resultate und Parameter der Methoden standardisiert und bleiben selbst durch eine Anpassung der Methodik unverändert. Die OCTAVE<sup>SM</sup>-Methodik ist jedoch nicht festgeschrieben und kann, ohne den OCTAVE<sup>SM</sup>-Ansatz zu verletzen, angepasst werden. Ebenso ist die Anwendung von in der OCTAVE<sup>SM</sup>-Methodik verwendeten Methoden nicht standardisiert.

### ***COBIT***

COBIT zeichnet sich durch ein hohes Maß an Standardisierung aus. COBIT basiert auf einer Vielzahl von internationalen Normen, Standards, Industriepraktiken und Kriterien für IT-Sicherheit und IT-Prozesse. Darunter sind unter anderem ISO Normen, ITSEC und CC zu finden. Somit ist die gesamte COBIT-Methodik auf diesen Normen und Standards aufgebaut, wobei sich die Audit Guidelines noch auf eventuelle lokale Voraussetzungen anpassen lassen.

### ***ISO/IEC 17799***

Die ISO/IEC 17799 stellt selbst einen Standard dar. Sie dient als Grundlage für die anderen Methodiken, und genießt einen wichtigen internationalen Status in praktisch allen Branchen.<sup>185</sup>

### ***Marion***

Marion benutzt standardisierte Interviews, Fragebögen und Maßnahmenkataloge und erfüllt somit das Kriterium der Standardisierung in der Verwendung von standardisierten Methoden. Internationale Anerkennung der Methodik ist kaum mehr gegeben, da die Methodik sich ursprünglich nur auf den frankophonen Raum konzentriert, und auch dort immer mehr an Bedeutung verliert. Die Darstellung der Resultate erfolgt standardisiert auf graphische Art.<sup>186</sup>

---

<sup>184</sup> [Vgl. Alberts & Dorofee 2002, Anhang C]

<sup>185</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 9f]

<sup>186</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 19f]

## Unabhängigkeit

### *BSI Grundschatz*

Die Durchführung der BSI-Grundschatz-Methodik ist vollständig unabhängig möglich.

### *OCTAVE<sup>SM</sup>*

Die OCTAVE<sup>SM</sup>-Methodik kann nicht nur unabhängig durchgeführt werden, Unabhängigkeit ist durch das OCTAVE<sup>SM</sup> Principle der Self Direction sogar direkt in die Methodik integriert.

### *COBIT*

Die Durchführung der COBIT-Methodik bzw. die IT-Control-Überprüfung kann unabhängig erfolgen, eine Durchführung der IT-Control-Überprüfung durch von der Organisation fremde Personen wird jedoch empfohlen. Zumindest sollte der Durchführende unabhängig von der überprüften Abteilung sein.<sup>187</sup>

### *ISO/IEC 17799*

Die Anwendung der ISO/IEC 17799 erfolgt in diesem Sinne unabhängig, dass die Einrichtung eines IT-Sicherheits-Systems in der Organisation durch die Organisation selbst erfolgen muss. Die IT-Sicherheits-Überprüfung nach dieser Norm kann sowohl unabhängig als auch durch Dritte erfolgen, wobei eine Zuhilfenahme von qualifiziertem externen Personal sinnvoll ist.

### *Marion*

Marion kann nach entsprechender Ausbildung durch firmeneigenes Personal durchgeführt werden.<sup>188</sup>

---

<sup>187</sup> [Vgl. IT Governance Institute, 2000e, S. 206ff]

<sup>188</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 21]

## Umsetzbarkeit

### *BSI Grundschutz*

Die BSI Grundschutz-Methodik liefert konkrete, praxisbezogene Maßnahmen, die sich gemäß dem Kriterium der Umsetzbarkeit unmittelbar umsetzen lassen. Die BSI Grundschutz-Methodik unterstützt die Umsetzung der Ergebnisse durch einen Umsetzungsplan.<sup>189</sup>

### *OCTAVE<sup>SM</sup>*

Die Ergebnisse von OCTAVE<sup>SM</sup> sind die Schutzstrategie, Risikolinderungspläne und eine Aktionsliste. Sie bilden verschiedene Ebenen der Umsetzbarkeit. Während die Schutzstrategie langfristige Aktionen beinhaltet und die Risikolinderungspläne mittelfristig orientiert sind, besteht die Aktionsliste aus unmittelbar umzusetzenden Maßnahmen.<sup>190</sup> Eine gute Umsetzbarkeit ist somit gewährleistet.

### *COBIT*

Durch den Einsatz der COBIT Audit Guidelines wird aufgezeigt, welche der Kontrollziele nicht erreicht wurden. Maßnahmen zur Erreichung der Kontrollziele werden nicht geboten. COBIT ist somit eher zur Überprüfung der IT-Control als zur Bestimmung praxisorientierter Maßnahmen geeignet.

### *ISO/IEC 17799*

Die ISO/IEC 17799 konzentriert sich ausschließlich auf konkrete praktische Maßnahmen, welche umgesetzt werden müssen. Theoretische Überlegungen bleiben größtenteils außen vor.<sup>191</sup>

### *Marion*

Marion liefert als Ergebnisse die IT-Sicherheitsschwächen der Organisation, und liefert standardisierte Maßnahmen aus einer Erfahrungsdatenbank. Diese werden durch funktionale An-

---

<sup>189</sup> [Vgl. GSHB, S. 77ff]

<sup>190</sup> [Vgl. Abschnitt 2.2.2]

<sup>191</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 8]

forderungen und mögliche Implementierungsvorschläge präsentiert. Diese sind zwar umfangreich, jedoch wenig konkret.<sup>192</sup>

### **Anpassungsfähigkeit/Skalierbarkeit**

#### ***BSI Grundschatz***

Die BSI Grundschatz-Methodik lässt sich dank ihres modulartigen Aufbaus in übergeordnete und spezifische Komponenten unabhängig von der Organisationsstruktur anwenden und zeichnet sich somit durch eine hervorragende Anpassungsfähigkeit aus.

#### ***OCTAVE<sup>SM</sup>***

Abgesehen von der OCTAVE<sup>SM</sup>-Variation OCTAVE<sup>SM</sup>-S lässt sich die OCTAVE<sup>SM</sup>-Methodik beliebig auf verschiedenste Organisationsstrukturen und –größen anpassen. Dies ist allerdings unter Umständen mit einigem Aufwand verbunden.<sup>193</sup>

#### ***COBIT***

COBIT erlaubt durch die Ansatzebenen des COBIT Cube die Skalierung auf einzelne IT-Domänen oder Business Requirements of Information. Auch das Herausgreifen einzelner IT-Prozesse ist möglich.

#### ***ISO/IEC 17799***

Die Anpassung der ISO/IEC 17799 an verschiedene Organisationen ist dank der übersichtlichen Struktur mit geringem Aufwand möglich. Weiters unterstützt wird dies durch den Einsatz von Softwarewerkzeugen.<sup>194</sup>

#### ***Marion***

Die 27 von Marion verwendeten Sicherheitsfaktoren können auf eigene Bedürfnisse angepasst werden. Organisationseigene Risiken können in die Methodik eingearbeitet werden.

---

<sup>192</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 19ff]

<sup>193</sup> [Vgl. Abschnitt 2.2.2]

Zusätzlich ist eine Ergänzung mit Sicherheitsfaktoren aus anderen Methodiken denkbar. Diese Aktionen verlangen aber einiges Geschick.<sup>195</sup>

### **Einfachheit der Anwendung und Tool-Unterstützung**

#### ***BSI Grundschatz***

Die Anwendung der BSI-Grundschatz-Methodik ist einigermaßen arbeitsintensiv und mit einigem Lernaufwand verbunden. Die IT-Sicherheits-Überprüfung mithilfe des GSHB ist als Soll-Ist-Vergleich einfach gestaltet und stellt keine hohen Anforderungen. Das BSI stellt mit dem BSI Grundschatztool ein Werkzeug zur Unterstützung der Anwendung zur Verfügung, welches die Anwendung erleichtert.<sup>196</sup> Auch inhaltlich stehen Werkzeuge zur Unterstützung der Methodik zur Verfügung. Die Werkzeuge unterliegen einer ständigen Weiterentwicklung.<sup>197</sup>

#### ***OCTAVE<sup>SM</sup>***

Die OCTAVE<sup>SM</sup>-Methodik ist in ihrer Anwendung mit erheblichem Aufwand verbunden. Durch die Selbststeuerung der Methodik ist auch der Lernaufwand des Personals erheblich. Werkzeuge werden nicht mit der Methodik geliefert, abgesehen von den nötigen Arbeitsmitteln. Es gibt jedoch Softwarewerkzeuge von externen Anbietern, welche beispielsweise die Datensammlung und -organisation vereinfachen. Ein Beispiel ist das OCTAVE®-Automated Tool des Advanced Technology Institutes.<sup>198</sup>

#### ***COBIT***

COBIT verlangt einen hohen Initialaufwand beim Anwender, welcher durch die nicht leicht verständliche Struktur der Methodik bedingt ist. Die Unterstützung der Methodik durch die

---

<sup>194</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 9]

<sup>195</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 21]

<sup>196</sup> [Vgl. Abschnitt 3.3.5]

<sup>197</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 26]

<sup>198</sup> [Vgl. OCTAVE<sup>SM</sup> Information Centre & ATI Corp., April 2005, 4, [http://oattool.aticorp.org/Tool\\_Info.html](http://oattool.aticorp.org/Tool_Info.html)]

Anwendung von Datenbanken oder Softwarewerkzeugen ist möglich, verschiedene Werkzeuge sind auf dem Markt verfügbar.

### ***ISO/IEC 17799***

Die ISO/IEC ist insbesondere durch den Einsatz von Softwarewerkzeugen, welche von verschiedenen Anbietern verfügbar sind, einfach anzuwenden.

### ***Marion***

Marion ist erst nach entsprechender Ausbildung durch organisationseigenes Personal durchführbar, wird allerdings durch eine leistungsfähige Software unterstützt.<sup>199</sup>

## **Beurteilungsumfang/Vollständigkeit**

### ***BSI Grundschutz***

Die BSI Grundschutz-Methodik ist definitionsgemäß auf das Erreichen eines angemessenen bzw. minimalen IT-Sicherheitsniveaus – den Grundschutz - ausgerichtet. Besondere Anforderungen an die IT-Sicherheit bedingen den Einsatz zusätzlicher, über den Grundschutz hinausgehende Maßnahmen.

### ***OCTAVE<sup>SM</sup>***

OCTAVE<sup>SM</sup> bietet eine umfassende IT-Sicherheits-Überprüfung mit Risikoanalyse und Schwachstellenanalyse. Organisatorische Aspekte werden ebenso behandelt wie technische. Die Tiefe der Betrachtung lässt sich je nach gewünschter Ergebnistiefe skalieren, eine freiwillige Einschränkung wird aber gemäß dem OCTAVE<sup>SM</sup> Attribute „Focus on the critical few“ empfohlen, um umsetzbarere Ergebnisse zu erzielen.

### ***COBIT***

Die COBIT Kontrollziele sind technikenunabhängig definiert, die Methodik konzentriert sich auf die IT-Governance, und erreicht so eine systemunabhängige Vollständigkeit. Ein durch

COBIT definiertes vollständiges Sicherheitsniveau gibt es nicht, der Fokus liegt auf den Unternehmenszielen.

### ***ISO/IEC 17799***

Vollständigkeit ist von der ISO/IEC 17799 nicht zu erwarten, da sie lediglich Grundschutzmaßnahmen anbietet. Organisationsspezifische Maßnahmen kommen nicht vor. Dementsprechend können zusätzliche Maßnahmen nötig sein, um die IT-Sicherheit zu komplettieren.<sup>200</sup>

### ***Marion***

Marion deckt die Bereiche der Risikoanalyse und der Erstellung eines IT-Sicherheitskonzeptes ab. Die Bearbeitungstiefe ist nicht skalierbar, da die verwendbaren Fragebögen vorgegeben sind.<sup>201</sup>

## **Präsentation der Ergebnisse**

### ***BSI Grundschutz***

Die Ergebnisse der BSI Grundschutz-Methodik erfolgt durch die Verwendung von mitgelieferten Formularen. Eine graphische Darstellung lässt die BSI Grundschutz-Methodik jedoch vermissen. Das BSI Grundschutztool<sup>202</sup> verbessert jedoch die Darstellung der Ergebnisse.

### ***OCTAVE<sup>SM</sup>***

Die Präsentation der Ergebnisse der OCTAVE<sup>SM</sup>-Methodik erfolgt in der Formulierung von Strategien, Plänen und Aktionen. Eine graphische Darstellung ist nicht vorgesehen.

---

<sup>199</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 19ff]

<sup>200</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 9f]

<sup>201</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 19ff]

<sup>202</sup> [Vgl. Abschnitt 3.3.5]

### ***COBIT***

COBIT liefert eine Reihe von Ergebnissen, im Bereich der IT-Control-Überprüfung sind die nicht erreichten Kontrollziele als Ergebnis zu werten. Die Darstellung der Ergebnisse erfolgt nicht in graphischer Form. Generell ist die Darstellung der Ergebnisse keine Stärke der COBIT-Methodik, sie kann jedoch durch den Einsatz von Softwarewerkzeugen verbessert werden.

### ***ISO/IEC 17799***

Die Darstellung der Ergebnisse wird bei der ISO/IEC 17799 erst durch den Einsatz von Softwarewerkzeugen in eine graphische Form gebracht. Ansonsten sind die Ergebnisse in Form von nicht implementierten Grundschutzmaßnahmen präsentiert, welche jedoch zu Bereichen zusammengefasst und dadurch auch relativ einfach graphisch aufbereitet werden können.<sup>203</sup>

### ***Marion***

Die Präsentation der Ergebnisse ist eine der Stärken der Marion-Methodik. Sie erfolgt graphisch in Form eines Rosettendiagramms. Dadurch lässt sich leicht die Homogenität bzw. Unhomogenität des IT-Sicherheitsniveaus ablesen.<sup>204</sup>

## **Effizienz**

### ***BSI Grundschutz***

Die Durchführung der BSI Grundschutzmethodik zur Etablierung ist mit einigem Arbeitsaufwand verbunden. Der Großteil der Kosten konzentriert sich bei organisatorischem und personellem Aufwand. Der Einsatz von kostenintensiven Dienstleistungen entfällt. Die

---

<sup>203</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 7ff]

<sup>204</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 20]

Grundschutzanalyse kann jedoch je nach der eingesetzten IT-Infrastruktur zeitaufwendig werden, und bewegt sich im Bereich von drei Monaten für eine mittelgroße Organisation.<sup>205</sup>

### ***OCTAVE<sup>SM</sup>***

Die OCTAVE<sup>SM</sup>-Methodik erfordert einigen Aufwand an Personal und Arbeitszeit. Die Zeitdauer zur Durchführung der OCTAVE<sup>SM</sup>-Methodik beträgt zwischen 2-3 Wochen und mehreren Monaten, je nach der Tiefe der Überprüfung und der Komplexität der nötigen Planung. Die Führung und die Teilnahme an den Workshops zieht zusätzlich noch Personal von ihren üblichen Aufgaben ab. Die Selbststeuerung der Methodik lässt den Erwerb von externen Dienstleistungen für den Großteil der IT-Sicherheits-Überprüfung entfallen. Unter Umständen kann jedoch externes Wissen von Nutzen sein, beispielsweise bei der Schwachstellenanalyse.

Die OCTAVE<sup>SM</sup>-S-Methodik ist durch ihre vereinfachte Form in entsprechend kürzerer Zeit durchführbar.

### ***COBIT***

Eine vollständige COBIT Analyse ist in einer mittelgroßen Organisation in etwa einem Arbeitsmonat abgeschlossen.<sup>206</sup>

### ***ISO/IEC 17799***

Durch die Einfachheit der Anwendung der ISO/IEC 17799 kann je nach Erfahrung des Personals innerhalb von einigen Wochen ein Maßnahmenkatalog erstellt werden.<sup>207</sup>

### ***Marion***

Marion ist sehr aufwandsintensiv, was als Nachteil der Methodik gewertet werden muss. Eine Dauer von ca. vier Monaten ist zu veranschlagen, und je nach Organisationsgröße benötigt die Anwendung von Marion erheblichen personellen Aufwand.<sup>208</sup>

---

<sup>205</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 24]

<sup>206</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 25]

<sup>207</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 9]

<sup>208</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 21]

## **Aktualität/Updatefrequenz**

### ***BSI Grundsatz***

Das BSI GS HB unterliegt einer ständigen Weiterentwicklung auf der Basis von Anwenderfeedback. Bezüglich Aktualität und Updatefrequenz bleiben wenige Wünsche offen. Die Entwicklung von sehr speziellen Bausteinen könnte jedoch möglicherweise durch den Anwender nötig sein.

### ***OCTAVE<sup>SM</sup>***

Es gibt keine regelmäßigen Updates für OCTAVE<sup>SM</sup>. Durch den Fokus auf die organisationsweite IT-Sicherheit auf Kosten der technologischen IT-Sicherheit sind Updates der Methodik an sich nicht nötig. Neuerungen in der IT müssen bei der Durchführung eingearbeitet werden, beispielsweise durch die Verwendung von aktuellen Werkzeugen bei der Schwachstellenanalyse.

### ***COBIT***

Die Updateaktivitäten von COBIT werden durch das Benutzerfeedback gesteuert und werden in der Veröffentlichung der vierten Edition einen neuen Höhepunkt finden. Durch die systemunabhängige Struktur sind jedoch aktuelle Updates keine Notwendigkeit für einen effizienten Einsatz der Methodik. Lediglich die Anwendung der Methodik wird durch Updates der Arbeitsmittel und Dokumente merklich gesteigert.

### ***ISO/IEC 17799***

Die ISO/IEC 17799 unterliegt als ISO Norm keinen häufigen Updates. Sie basiert auf der britischen Norm BS 7799 und wurde 2000 zur ISO Norm erweitert. Die neueste Ausgabe stammt aus dem Jahr 2001, und ist zurzeit zur Revision ausgeschrieben.<sup>209</sup>

---

<sup>209</sup> [Vgl. ISO, April 2005, 5, ISO/IEC 17799:2000, <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=&showrevision=y>]

### ***Marion***

Regelmäßige Updates beschränken sich bei der Marion-Methodik auf die verwendeten Fragebögen. Durch den Verlust ihrer Bedeutung sind keine Veränderungen der Methodik an sich mehr zu erwarten.<sup>210</sup>

### **Zertifizierbarkeit**

#### ***BSI Grundschutz***

Organisationen können mit einem BSI Grundschutzzertifikat die Umsetzung der Grundschutzmaßnahmen nachweisen. Dies geschieht durch einen Basis-Sicherheitscheck, welcher von einer unabhängigen, akkreditierten Stelle durchgeführt wird.<sup>211</sup>

#### ***OCTAVE<sup>SM</sup>***

Eine Zertifizierung der OCTAVE<sup>SM</sup>-Methodik ist nicht vorgesehen.

#### ***COBIT***

Ein Zertifikat für Anwender der COBIT-Methodik gibt es nicht. Die COBIT-Methodik wird jedoch von vielen Wirtschaftsprüfungsunternehmen eingesetzt, um die IT-Control ihrer Kunden zu überprüfen.<sup>212</sup>

#### ***ISO/IEC 17799***

Die Zertifizierbarkeit nach ISO/IEC 17799 ist durch verschiedene Institutionen möglich, u.a. durch das BSI.<sup>213</sup>

---

<sup>210</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 21f]

<sup>211</sup> [Vgl. GSHB, S. 82]

<sup>212</sup> [Vgl. Initi@tive D<sup>21</sup>, 2001, S. 31]

<sup>213</sup> [Vgl. ISO 17799 Information Security Group, April 2005, 6, ISO 17799 FAQ, <http://www.iso-17799.com/faq.htm>]

### *Marion*

Die Zertifizierbarkeit ist eine weitere Schwäche von Marion. Es ist durch die Art der Methodik nicht sichergestellt, dass eine erneute Durchführung der Methodik zu denselben Ergebnissen kommt. Die Erstellung der neuen Fragebögen erfolgt auf Französisch; erst im Anschluss erfolgt eine englische Übersetzung, welche erfahrungsgemäß eher mäßig ausfällt.<sup>214</sup>

---

<sup>214</sup> [Vgl. ISACA Switzerland Chapter, 1998, S. 21]

### 3 Methoden und Werkzeuge zur IT-Sicherheits-Überprüfung

Die im vorangegangenen Kapitel vorgestellten Methodiken stellen ganzheitliche Ansätze dar, um die IT-Sicherheit zu erlangen und mittels Prüfungsverfahren sicherzustellen. Im Zuge dieser IT-Sicherheits-Überprüfungen ist der Einsatz von unterschiedlichen Methoden nötig, welche wiederum den Einsatz von (Software)-Werkzeugen benötigen. Diesen Methoden und Werkzeugen widmet sich die vorliegende Arbeit in diesem Kapitel.

#### 3.1 Penetrationstest

Der Penetrationstest dient dazu, die momentane Gefährdung eines IT-Systems durch Angreifer festzustellen, bzw. zu ermitteln, ob die aktuell eingesetzten IT-Sicherheitsmaßnahmen ausreichend sind.<sup>215</sup> Penetrationstests sind direkt auf das Aufdecken und Ausnutzen von angreifbaren Schwachstellen ausgerichtet, und überprüfen sowohl logische als auch physische IT-Sicherheitsmaßnahmen.<sup>216</sup> Die Betrachtung des Penetrationstests erfolgt anhand einer Studie des BSI zur Durchführung von Penetrationstests. Eine Reihe von Zielsetzungen können durch einen Penetrationstest erfüllt werden:<sup>217</sup>

- Erhöhung der IT-Sicherheit technischer Systeme: Erkennen von Schwachstellen und Beseitigen derselben
- Identifikation von Schwachstellen: Ausschließlich das Erkennen von Schwachstellen, um beispielsweise vor einem Zusammenschluss von zwei IT-Netzwerken bei der Feststellung von Schwachstellen in einem der beiden abzusehen
- Bestätigung der IT-Sicherheit durch einen externen Dritten: Demonstration von ausreichenden Sicherheitsmaßnahmen gegenüber den Kunden der Organisation oder ähnliches
- Erhöhung der Sicherheit der personellen und organisatorischen Infrastruktur: Test von Eskalationsprozeduren, Sicherheitsbewusstsein des Personals und Wirksamkeit von IT-Sicherheitspolitiken

Im Ergebnis eines Penetrationstests sollten daher nicht nur eine Auflistung von Schwachstellen, sondern ebenfalls Lösungs- und Verbesserungsvorschläge enthalten sein.<sup>218</sup>

Ein Penetrationstest stellt immer eine Momentaufnahme dar, das IT-Sicherheitsniveau in der Zukunft kann aus ihnen nicht abgelesen werden. Dies ist allein schon durch die ständige Entdeckung von neuen Schwachstellen gegeben.<sup>219</sup>

---

<sup>215</sup> [Vgl. BSI, 2003, S. 5]

<sup>216</sup> [Vgl. BSI, 2003, S. 10]

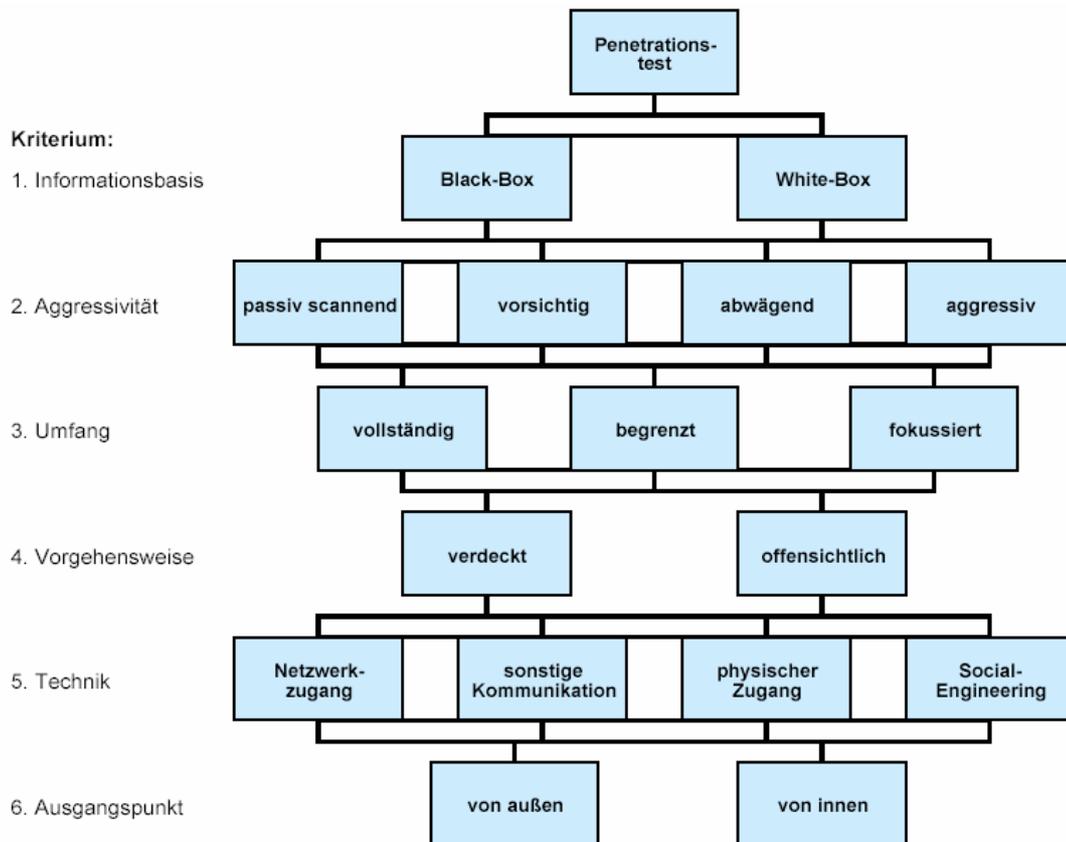
<sup>217</sup> [Vgl. BSI, 2003, S. 10f]

<sup>218</sup> [Vgl. BSI, 2003, S. 11]

Bei einem Penetrationstest müssen immer gewisse Rahmenbedingungen wie ethische Überlegungen oder gesetzliche Bestimmungen beachtet werden.<sup>220</sup>

### 3.1.1 Klassifikation von Penetrationstests

Penetrationstests können auf verschiedene Art und Weise durchgeführt werden. Verschiedene Kriterien bilden den Unterschied zwischen einem Penetrationstest und einem anderen Penetrationstest. Die Unterscheidungsmerkmale, welche in Abbildung 3-1 dargestellt werden, müssen je nach Aufgabenstellung angepasst werden.



**Abbildung 3-1: Klassifikation von Penetrationstests**

Quelle: BSI 2003, S. 13

Bei der Anpassung an die Zielsetzung ist zu beachten, dass nicht alle Kombinationen der Kriterien sinnvoll sind. Aggressives Vorgehen ist mit einer verdeckten Vorgehensweise nicht gut vereinbar.<sup>221</sup>

<sup>219</sup> [Vgl. BSI, 2003, S. 12]

<sup>220</sup> [Vgl. BSI, 2003, S. 18ff]

<sup>221</sup> [Vgl. BSI, 2003, S. 13]

In der Folge werden die Kriterien der Klassifikation von Penetrationstests und deren mögliche Werte erläutert.

### **Informationsbasis**

Das Kriterium der Informationsbasis beschreibt, von welchem Wissensstand über das Zielobjekt bzw. Zielnetzwerk der Penetrationstester ausgeht.

Ein **Black-Box**-Test entspricht einem Angriff durch organisationsfremde, externe Angreifer. Kein Wissen über die internen Strukturen wird vorausgesetzt, der Penetrationstester muss alle Informationen aus öffentlich zugänglichen Datenbanken recherchieren oder als organisationsfremde Person zu erfragen versuchen.<sup>222</sup>

Im Gegensatz dazu bekommt der Penetrationstester bei einem **White-Box**-Test vorab Informationen über das Ziel zur Verfügung gestellt. Dies entspricht einer Angriffssituation, wie sie ein (ehemaliger) Mitarbeiter der Organisation vorfindet. Die Tiefe der Hintergrundinformationen kann stufenlos angepasst werden, um verschiedene Angreifer zu simulieren.<sup>223</sup>

### **Aggressivität**

Die Aggressivität des Penetrationstests bestimmt, wie aggressiv der Penetrationstester bei seinen Angriffsversuchen vorgeht. Mehrere Aggressivitätsstufen sind möglich.

In der niedrigsten Stufe erfolgt die Untersuchung der Zielobjekte nur **passiv**. Gefundene Schwachstellen werden nicht ausgenutzt.<sup>224</sup>

In der nächsten Stufe – vorsichtig - werden Sicherheitsschwächen nur ausgenutzt, wenn eine Beeinträchtigung der Funktion des Zielobjektes ausgeschlossen werden kann.<sup>225</sup>

In der dritten Stufe der Aggressivität verhält sich der Penetrationstester **abwägend**; Schwachstellen werden auch ausgenutzt, wenn Systembeeinträchtigungen möglich sind. Die Erfolgsaussichten und möglichen Konsequenzen werden aber davor gegeneinander abgewogen.<sup>226</sup>

---

<sup>222</sup> [Vgl. BSI, 2003, S. 13]

<sup>223</sup> [Vgl. BSI, 2003, S. 14]

<sup>224</sup> [Vgl. BSI, 2003, S. 14]

<sup>225</sup> [Vgl. BSI, 2003, S. 14]

<sup>226</sup> [Vgl. BSI, 2003, S. 14]

Die höchste Aggressivitätsstufe beschreibt ein Vorgehen, bei dem der Penetrationstester das Zielsystem **aggressiv** angreift. Alle potentiellen Schwachstellen werden ausgenutzt, auf mögliche Folgen wird keine Rücksicht genommen. Dies kann zum Ausfall der Zielobjekte oder benachbarter Systeme führen.<sup>227</sup>

#### Umfang

Der Umfang des Penetrationstests legt fest, welche IT-Systeme getestet werden sollen.

Ist der Penetrationstest **fokussiert**, werden nur ein bestimmtes Teilnetz, System oder ein bestimmter Dienst überprüft. Die Ergebnisse dieser Art von Penetrationstest sind dementsprechend nur eingeschränkt.<sup>228</sup>

Ein **begrenzter** Penetrationstest untersucht eine begrenzte Zahl von Systemen oder Diensten, beispielsweise alle Systeme eines funktionalen Verbundes oder alle Systeme der DMZ.<sup>229</sup>

Bei einem **vollständigen** Penetrationstest werden alle erreichbaren Systeme geprüft. Ausgenommen sind eventuell externe Systeme unter fremder Administration.<sup>230</sup>

#### Vorgehensweise

Die Vorgehensweise bestimmt, wie sichtbar der Penetrationstester vorgeht. Für den Test von gewissen IT-Sicherheitsmaßnahmen und –prozeduren muss die Vorgehensweise angepasst werden. Dies gilt beispielsweise für die Überprüfung eines IDS oder Incident Handling Prozeduren.

Ein **verdeckter** Penetrationstest ist nötig, um auch sekundäre Sicherheitssysteme und Eskalationsprozeduren zu testen. Das bedeutet, dass nur Methoden zur Erkundung eingesetzt werden, die nicht direkt als Angriffsversuche erkennbar sind.<sup>231</sup>

Falls durch den verdeckten Test keine Reaktionen provoziert wurden oder ein White-Box-Test durchgeführt wird, können auch **offensichtliche** Methoden eingesetzt werden. Ein offensichtlicher White-Box-Test hat auch den Vorteil, dass organisationseigenes Personal bei

---

<sup>227</sup> [Vgl. BSI, 2003, S. 14]

<sup>228</sup> [Vgl. BSI, 2003, S. 15]

<sup>229</sup> [Vgl. BSI, 2003, S. 15]

<sup>230</sup> [Vgl. BSI, 2003, S. 15]

<sup>231</sup> [Vgl. BSI, 2003, S. 15]

den Tests anwesend sein kann, um gegebenenfalls schnell auf unvorhergesehene Probleme reagieren zu können.<sup>232</sup>

#### **Technik**

Bei einem Penetrationstest können verschiedene Techniken eingesetzt werden. Klassisch erfolgt ein Angriff über das Netzwerk. Jedoch existieren noch andere Techniken.

Ein Penetrationstest über das **Netzwerk** entspricht dem üblichen Vorgehen und simuliert einen Hackerangriff. Zumeist erfolgt der Angriff über TCP/IP.<sup>233</sup>

Abgesehen von TCP/IP-Netzen gibt es **weitere Kommunikationsnetze**, über die ein Angriff erfolgen kann. Dazu zählen Telefon- und Faxnetze, sowie drahtlose Verbindungen.<sup>234</sup>

Durch die in modernen IT-Netzwerken oftmals eingesetzten IT-Sicherheitsmaßnahmen wie Firewalls oder IDS ist es oftmals einfacher, direkten **physischen Zugriff** auf das Zielsystem zu erlangen. Dies verlangt meist das Erlangen von unberechtigtem Zutritt in die Gebäude und Räume der Organisation.<sup>235</sup>

Die letzte Technik, welche bei Penetrationstechniken eingesetzt wird, ist **Social Engineering**. Diese Technik nutzt den Menschen als schwächstes Glied der IT-Sicherheitskette aus. Das Personal einer Organisation hat oftmals unzureichende Sicherheitskenntnisse oder ein geringes Sicherheitsbewusstsein. Durch Social Engineering kann der Grad der Akzeptanz von neuen Sicherheitspolitiken geprüft werden.<sup>236</sup>

#### **Ausgangspunkt**

Das letzte Kriterium zur Klassifikation ist der Ausgangspunkt, welcher definiert, von wo aus der Penetrationstest durchgeführt wird. Dies ist der Punkt, an dem der Penetrationstester seinen Rechner ans Netz anschließt.

---

<sup>232</sup> [Vgl. BSI, 2003, S. 15]

<sup>233</sup> [Vgl. BSI, 2003, S. 16]

<sup>234</sup> [Vgl. BSI, 2003, S. 16]

<sup>235</sup> [Vgl. BSI, 2003, S. 16]

<sup>236</sup> [Vgl. BSI, 2003, S. 16]

Penetrationstests **von außen** können bestimmen, was ein Angreifer ohne Zugriff auf das interne Netzwerk erreichen kann. Ansatzpunkt für solche Angriffe sind meist die Firewall oder die IT-Systeme in der DMZ.<sup>237</sup>

Erfolgt ein Penetrationstest **von innen**, kann überprüft werden, was ein Angreifer von außen nach der Überwindung der Firewall bzw. ein Angreifer mit Zugriff auf das interne Netz erreichen kann.<sup>238</sup>

#### 3.1.2 Methodik für die Durchführung von Penetrationstests

Die Methodik zur Durchführung von Penetrationstest des BSI ist in fünf Phasen gegliedert und folgt einem Modulaufbau in den einzelnen Phasen.<sup>239</sup>

##### **Phase 1: Vorbereitung**

In der Vorbereitung erfolgt zuerst die Zielsetzung des Penetrationstests, um den Wünschen des Auftraggebers gerecht zu werden. Darüber hinaus müssen mögliche Folgen, wie etwa Produktionsausfälle, mit dem Auftraggeber besprochen werden und alle nötigen Details vertraglich festgehalten werden. Die Beachtung aller gesetzlichen Rahmenbedingungen ist zu beachten.<sup>240</sup>

##### **Phase 2: Informationsbeschaffung und -auswertung**

Ziel von Phase 2 ist es, eine möglichst komplette und detaillierte Übersicht über die installierten Systeme und mögliche Angriffspunkte und bekannte Sicherheitsmängel zu erlangen. Laufende Betriebssysteme und Dienste werden ermittelt. Dies kann mitunter eine lange Zeit in Anspruch nehmen.<sup>241</sup>

##### **Phase 3: Bewertung der Informationen / Risikoanalyse**

Um den Penetrationstest effizient und wirtschaftlich zu halten, müssen die gesammelten Informationen ausgewertet werden. Schwachstellen der laufenden IT-Systeme, Dienste und Betriebssysteme werden bestimmt. Dadurch erreicht man, dass die zeitaufwendigen folgenden Prüfungsschritte fokussiert werden. Die Angriffsziele für das aktive Eindringen werden aus-

---

<sup>237</sup> [Vgl. BSI, 2003, S. 16]

<sup>238</sup> [Vgl. BSI, 2003, S. 17]

<sup>239</sup> [Vgl. BSI, 2003, S. 44]

<sup>240</sup> [Vgl. BSI, 2003, S. 45]

gewählt. Dies muss dokumentiert werden, da diese Auswahl zwar einerseits die Effizienz steigert, andererseits aber auch die Aussagekraft des Penetrationstests vermindert.<sup>242</sup>

#### **Phase 4: Aktive Eindringversuche**

Nun folgt der Angriff auf die ausgewählten Systeme. Dies ist mit der nötigen Sorgfalt durchzuführen, da dies die Phase mit dem größten Risiko ist. Hier wird aufgedeckt, inwieweit die in Phase 2 identifizierten möglichen Schwachstellen tatsächlich Sicherheitsmängel darstellen. Bei kritischen Systemen muss das Risiko eines Ausfalls immer genau abgewogen werden. Das Einspielen von eventuell verfügbaren Patches bei vermeintlichen Sicherheitsschwächen verhindert zwar möglicherweise das Entdecken einer Schwachstelle, dokumentiert dafür die Sicherheit des Systems nach dem Update.<sup>243</sup>

#### **Phase 5: Abschlussanalyse**

Im Rahmen der Abschlussanalyse werden die gefundenen Schwachstellen in Form der potentiellen Risiken und Empfehlungen zur Kompensation dokumentiert. Im Abschlussbericht sind die einzelnen Prüfungsschritte und Ergebnisse nachvollziehbar darzustellen.<sup>244</sup>

In Abbildung 3-2 wird die Vorgehensweise bei der Durchführung eines Penetrationstests dargestellt.

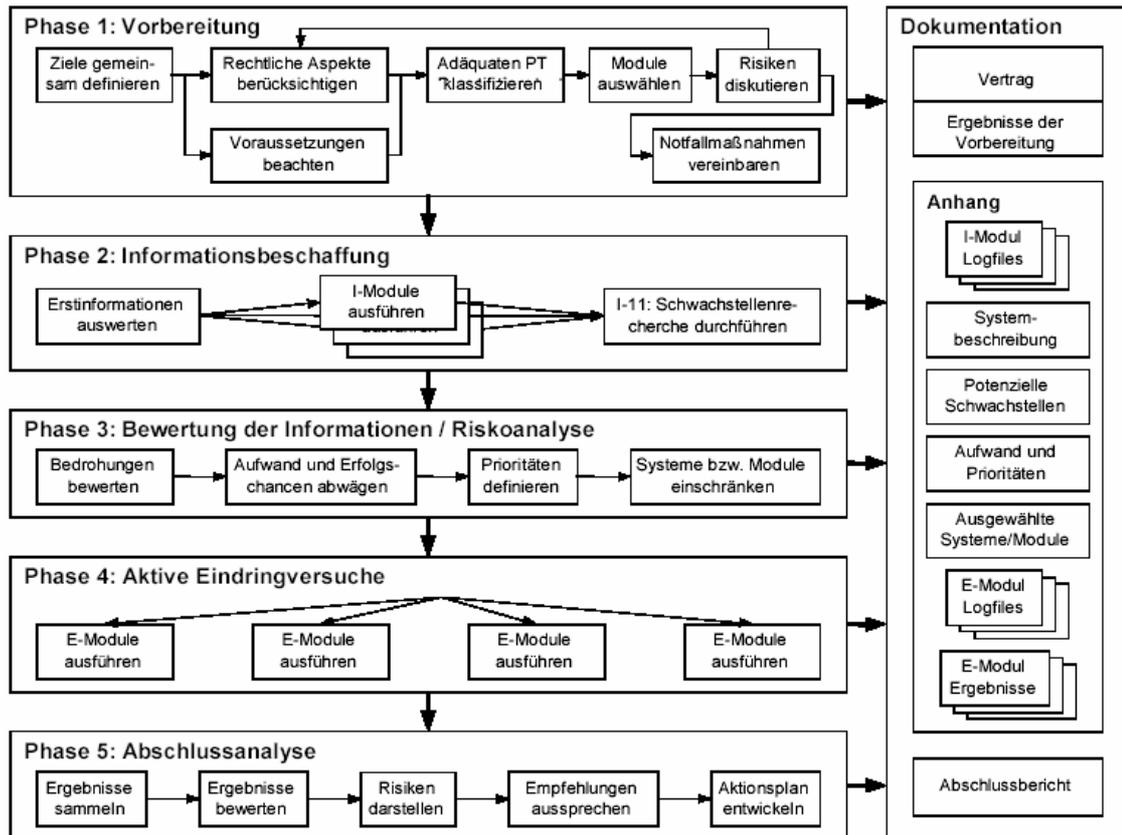
---

<sup>241</sup> [Vgl. BSI, 2003, S. 45]

<sup>242</sup> [Vgl. BSI, 2003, S. 45f]

<sup>243</sup> [Vgl. BSI, 2003, S. 46]

<sup>244</sup> [Vgl. BSI, 2003, S. 46]



**Abbildung 3-2: Fünfphasige Vorgehensweise bei Penetrationstests**

Quelle: BSI 2003, S. 47

In der Vorgehensweise sind keine expliziten Prüfungshandlungen vorgeschrieben. Stattdessen wird die Ausführung der Module aus zwei Klassen – die I-Module und die E-Module - definiert. Die I-Module dienen der Informationsbeschaffung, die E-Module stellen Eindringversuche dar. Für eine Liste der Module siehe Anhang G der vorliegenden Arbeit.

### Dokumentation

Begleitend zu den einzelnen Phasen ist die Dokumentation der einzelnen Aktionen nötig. Die Dokumentation sollte nicht erst nach Abschluss des Penetrationstests erstellt werden. Umfang und Inhalt der Dokumentation des Penetrationstests müssen vertraglich vereinbart werden. Folgende Inhalte sind möglich:<sup>245</sup>

- Der Vertrag inkl. aller Vereinbarungen
- Die Dokumentation aller durchgeführten Schritte zur Informationsbeschaffung, die Logfiles der eingesetzten Werkzeuge einschließlich der Liste der geprüften Schwachstellen

<sup>245</sup> [Vgl. BSI, 2003, S. 99]

- Die daraus abgeleiteten Systembeschreibungen
- Liste der potentiellen Schwachstellen, aufgeschlüsselt nach System und einschließlich einer Kurzbeschreibung
- Die Ergebnisse der Risikoanalyse und die damit ausgewählten Systeme bzw. E-Module für Phase 4
- Die Dokumentation der abgearbeiteten E-Module und die Logfiles der eingesetzten Werkzeuge
- Die einzelnen Ergebnisse der E-Module einschließlich der Liste der durch sie bestätigten Schwachstellen
- Ein Abschlussbericht

Üblicherweise erfolgen abschließend die Präsentation der Ergebnisse und das Aussprechen von Empfehlungen an den Auftraggeber des Penetrationstests.

### 3.2 Security Compliance Check

Der Security Compliance Check dient der Überprüfung, ob die eingesetzten IT-Sicherheitsmaßnahmen mit der IT-Sicherheitspolitik und dem IT-Sicherheitsplan übereinstimmen. Dies ist nötig, um das erreichte Sicherheitsniveau aufrecht zu erhalten. Dies muss für alle IT-Systeme, -Projekte und Applikationen gewährleistet sein. Darüber hinaus dient der Security Compliance Check dazu, die Übereinstimmung der IT-Sicherheitsmaßnahmen mit gesetzlichen und betrieblichen Vorgaben zu bestätigen.<sup>246</sup>

Ein Security Compliance Check ist notwendig.<sup>247</sup>

- Nach der Implementierung von neuen IT-Systemen oder Applikationen
- Nach eine in der IT-Sicherheitspolitik festgelegten Zeitspanne für alle in Betrieb befindlichen IT-Systeme und Applikationen

Security Compliance Checks können sowohl durch interne als auch externe Prüfer durchgeführt werden. Die Erstellung bzw. Benutzung von Checklisten ist empfohlen, um das Prüfverfahren zumindest innerhalb der Organisation zu standardisieren.

Anschließend folgt eine Beschreibung der nötigen Aktionen während eines Security Compliance Checks.

---

<sup>246</sup> [Vgl. Ö-IT-SIHB, Teil 2, S. 209]

<sup>247</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 209]

### 3.2.1 Überprüfung der Einhaltung von rechtlichen und betrieblichen Vorgaben

Zur Erfüllung dieses Punktes muss regelmäßig überprüft werden, ob die Systeme allen (insbesondere neuer) rechtlichen und betrieblichen Bestimmungen entsprechen, sowie ob die Vorgaben im tatsächlichen Betrieb auch eingehalten werden. Vorgaben, die es einzuhalten gilt, sind beispielsweise das DSGVO, gesetzliche Aufbewahrungs- und Löschfristen, Urheberrecht und Wettbewerbsgesetze.<sup>248</sup>

### 3.2.2 Überprüfung auf Einhaltung der Sicherheitspolitiken

Die Überprüfung auf Einhaltung der Sicherheitspolitiken ist ein Kernpunkt des Security Compliance Checks. Dies schließt folgende Teilmaßnahmen mit ein.<sup>249</sup>

- Regelmäßige Kontrolle, ob alle IT-Sicherheitsmaßnahmen und –vorgaben, die durch die IT-Sicherheitspolitik und IT-Systemsicherheitspolitiken festgelegt sind, vollständig und korrekt umgesetzt wurden
- Gewährleistung des korrekten Einsatzes der implementierten Sicherheitsmaßnahmen durch Stichproben
- Prüfung der Akzeptanz und Einhaltung der Sicherheitsvorgaben im täglichen Betrieb

Diese Überprüfungen erfordern Sachkenntnis und Kenntnis des zu prüfenden IT-Systems, den eingesetzten IT-Sicherheitsmaßnahmen und möglicher Bedrohungen.<sup>250</sup>

### 3.2.3 Auswertung von Protokolldateien

Die Protokollierung von Daten ist sicherheitstechnisch nur effizient, wenn die Protokolldaten auch ausgewertet werden. Dies muss in regelmäßigen Abständen geschehen. Dies sollte, wenn möglich, durch einen unabhängigen Revisor geschehen, da eine Auswertung durch den Systemadministrator das Risiko birgt, dass die Tätigkeiten des Systemadministrators selbst nicht kontrolliert werden.<sup>251</sup>

Bei der Kontrolle der Protokolldateien sollte man auf folgende Auswertungskriterien achten:<sup>252</sup>

- An- und Abmeldeversuche außerhalb der Arbeitszeit
- Häufung von fehlerhaften Anmeldeversuchen

---

<sup>248</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 209]

<sup>249</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 210]

<sup>250</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 210]

<sup>251</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 210]

<sup>252</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 210f]

- Häufung unzulässiger Zugriffsversuche
- Größere Zeitintervalle ohne Protokollierung (vermutlich gelöschte Protokolle)
- Zu großer Umfang der protokollierten Daten (erschwert die Auswertung)
- Auffällig große Zeitintervalle ohne Benutzerwechsel (welche darauf schließen lassen, dass sich Benutzer nicht ordnungsgemäß abmelden)

Bei der Auswertung der in großen Mengen anfallenden Protokolldateien ist die Verwendung von Softwarewerkzeugen hilfreich. Für weitere Informationen bezüglich dieser Werkzeuge s. Abschnitt 3.3.4 der vorliegenden Arbeit.

### 3.2.4 Kontrolle bestehender Verbindungen

Alle Netzwerkkomponenten müssen einer zumindest stichprobenartigen Sichtprobe unterzogen werden. Folgenden Aspekten muss man dabei Beachtung schenken:<sup>253</sup>

- Spuren gewaltsamer Öffnungsversuche an verschlossenen Netzwerkverteilern
- Aktualität der in den Verteilern befindlichen Dokumentation der Netzwerkverbindungen
- Korrektheit der Dokumentation
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen
- Unzulässige Einbauten und Veränderungen

Abgesehen von der Sichtkontrolle sollte auch eine funktionale Kontrolle durchgeführt werden, welche bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte überprüft. Dies ist für selten genutzte Verbindungen und Verbindungen, über die oft kritische Daten übertragen werden, angebracht; also überall dort, wo Manipulationen nicht gut erkennbar bzw. mit schwerwiegenden Folgen verbunden sein können.<sup>254</sup>

### 3.2.5 Durchführung von Sicherheitskontrollen in Client-Server-Netzen

Folgende Kontrollen sollten auf Server-Ebene regelmäßig durchgeführt werden:<sup>255</sup>

- Prüfung der Korrektheit der sicherheitsrelevanten Systemeinstellungen
- Die Benutzung von privilegierten Benutzerkonten (Systemadministrator u.a.) durch Überprüfung der Protokolleinträge

---

<sup>253</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 211]

<sup>254</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 211]

<sup>255</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 212]

- Fehlgeschlagene Zugriffsversuche; bei Entdeckung von Berechtigungsverstößen ist die Ursache zu ermitteln
- Systemintegrität; insbesondere die Daten der letzten Veränderung und die Zugriffsrechte der wichtigen Systemdateien sollten mit den Aufzeichnungen der jeweils vorigen Überprüfung verglichen werden
- Unbenutzte Benutzerkonten; Berechtigungen ehemaliger Benutzer sollten sofort deaktiviert und nach einer Übergangszeit gelöscht werden. Die Liste der Benutzer ist regelmäßig zu überprüfen, um sicherzustellen, dass nur berechtigte Benutzer das System benutzen.
- Benutzer- und Gruppenberechtigungen; Gruppenmitgliedschaften müssen geprüft werden, wenn sich die Mitgliedschaft oder Aufgabe eines Benutzers ändert. Das Anhäufen von Berechtigungen muss auf diese Art verhindert werden. Spezialberechtigungen für Benutzer müssen regelmäßig mit den Vorgaben abgeglichen werden.
- Berechtigungskontrolle; Eigentümer von Dateien und Verzeichnissen haben die Verpflichtung, anderen nur Zugriff auf ihre Daten zu gewähren, wenn dies erforderlich ist. Die Einhaltung dieser Verpflichtung ist zu kontrollieren

#### 3.2.6 Kontrollgänge

Regelmäßige Kontrollgänge sind ein weiteres Instrument des Security Compliance Checks. Sie bieten ein einfaches und wirksames Mittel, die Einhaltung der IT-Sicherheitspolitiken und IT-Sicherheitsmaßnahmen zu prüfen. Bei Kontrollgängen ist darauf zu achten, dass sie auf das vorzeitige Beheben von Sicherheitsmängeln und nicht auf das Finden von Schuldigen ausgerichtet sind. Sie sind sowohl während als auch außerhalb der Dienstzeiten durchzuführen.<sup>256</sup>

#### 3.3 Werkzeuge der IT-Sicherheits-Überprüfung

Zur Unterstützung der Durchführung von IT-Sicherheits-Überprüfungen gibt es verschiedene Klassen von Werkzeugen. Manche dienen der Informationsbeschaffung, andere entdecken Schwachstellen und wieder andere helfen bei der Anwendung einer Methodik zur IT-Sicherheits-Überprüfung. Werkzeuge sind zu einem unabdingbaren Faktor in der IT-Sicherheit geworden, da sie den Aufwand begrenzen und das für ein relativ gutes Ergebnis nötige Know-How verringern. Ein gutes Werkzeug ersetzt jedoch keineswegs einen fähigen Anwender. Nur wer das nötige Fachwissen mitbringt, kann ein Werkzeug bestmöglich nutzen. In der Folge werden die verschiedenen Klassen von Werkzeugen beschrieben und gängige Vertreter dieser Klassen vorgestellt.

---

<sup>256</sup> [Vgl. Ö-IT-SIHB, Teil 1, S. 213]

### 3.3.1 Portscanner

Portscanner sind Werkzeuge, welche durch das geschickte Versenden von IP-Paketen eine Vielzahl von Informationen über ein Zielsystem bzw. Zielnetzwerk gewinnen können. Die grundlegende Funktion eines Portscanners ist das Finden von offenen Ports bzw. laufenden Diensten auf dem Zielsystem. Es gibt jedoch Portscanner, die viel mehr können als das. Verschiedene Scanningmethoden erlauben ein besonders vorsichtiges oder aggressives Vorgehen, andere Zusatzfunktionen erkennen das auf dem System laufende Betriebssystem (= OS Fingerprinting). Portscanner sind ein unentbehrliches Werkzeug für die Informationsbeschaffung bei der Durchführung von Penetrationstests. Die umfangreichen Funktionen, welche ein Portscanner bietet, werden nun anhand des wohl mächtigsten und meist benutzten Portscanners überhaupt – nmap - erläutert.

#### **nmap**

Nmap ist eine Entwicklung von Fyodor und wird dank der Offenlegung des Quellcodes von der Internetgemeinde weiterentwickelt. Nmap ist frei zum Download verfügbar. Nmap unterstützt verschiedenste fortgeschrittene Methoden zur Netzwerkanalyse. Dies beinhaltet mehrere Portscan-Mechanismen, OS Fingerprinting, Versionserkennung, Ping Sweeps und mehr. Nmap kann Netzwerke mit mehreren Hunderttausend Rechnern scannen und unterstützt eine Vielzahl an Plattformen, darunter Linux, Microsoft Windows, FreeBSD, Solaris, Mac OS X, HP-UX, NetBSD, Sun OS und OpenBSD. Trotz der weitreichenden Konfigurationsmöglichkeiten ist nmap einfach zu benutzen, und das sowohl in der Kommandozeile als auch als grafische Version. Eine äußerst umfangreiche man-page sowie Tutorials und zusätzliche Veröffentlichungen unterstützen Anfänger beim Erlernen der Arbeit mit nmap.<sup>257</sup> Nmap und Dokumentation zu allen Funktionen sind erhältlich auf <http://www.insecure.org/nmap/index.html>. Im Anschluss werden die verschiedenen Funktionen von nmap beschrieben.

#### ***Portscanning***

Nmap unterstützt verschiedene ausgefeilte Techniken des Portscans. Die Urform des Portscans ist der TCP-Connect Scan. Dabei versucht nmap (bzw. ein anderer Portscanner), eine Verbindung mit dem Zielpport aufzubauen. Gelingt dies, so ist der entsprechende Port natürlich geöffnet. Aufbauend auf dieser Technik bietet nmap eine Vielzahl von Scans. Sie alle

haben ihre Vor- und Nachteile. Die Aggressivität des Scans ist in mehreren Stufen einstellbar.<sup>258</sup> Die Portscan-Funktion von nmap ist so umfangreich, dass eine umfassende Beschreibung den Rahmen dieser Arbeit sprengen würde.

### ***OS Detection***

Eine andere Funktion von nmap erlaubt es, das laufende System auf dem Zielrechner zu identifizieren. Dies geschieht mittels OS Fingerprinting. Anhand der TCP/IP-Pakete, welche das Zielsystem nach bestimmten Aktionen des Scanners sendet, kann man auf das Betriebssystem rückschließen.<sup>259</sup> An dieser Stelle ist es ausreichend, zu sagen, dass nmap diese Funktion bietet. Für eine genauere Beschreibung siehe <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>.

### ***Version Detection***

Die Version Detection-Funktion von nmap erlaubt es dem Scanner, die Dienste, welche an den offenen Ports laufen, zu identifizieren und sogar die laufende Version des Dienstes zu ermitteln. Dies hilft bei der Identifizierung von möglichen Schwachstellen der Dienste. Nmap schafft die Version Detection durch das Senden von sog. „Probes“, welche einem Dienst, der die betreffende Probe versteht, die nötigen Informationen entlockt. Dies geht sogar soweit, dass nmap sich auf einem SSL-Port mit OpenSSL verbindet und versucht den Dienst hinter der Verschlüsselung zu identifizieren.<sup>260</sup> Für alle Version Detection-Funktionen siehe <http://www.insecure.org/nmap/versionscan.html>.

### **Andere Portscanner**

Nmap ist zwar das herausragende Beispiel der Portscanner, es gibt jedoch noch einige andere Portscanner mit umfangreichen Funktionen. Eine Beschreibung dieser Werkzeuge findet an dieser Stelle keinen Platz, für einige Beispiele jedoch schon:

- hping: umfassend konfigurierbarer Portscanner und Packet Generator/Packet Analyzer. Derzeit aktuell ist hping2, hping3 befindet sich in der Entwicklung. Quelle: <http://www.hping.org>

---

<sup>257</sup> [Vgl. Insecure.org, 2005, 7, <http://www.insecure.org/nmap/index.html>]

<sup>258</sup> [Vgl. Insecure.org, 2005, 7, [http://www.insecure.org/nmap/data/nmap\\_manpage.html](http://www.insecure.org/nmap/data/nmap_manpage.html)]

<sup>259</sup> [Vgl. Insecure.org, 2005, 7, <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>]

<sup>260</sup> [Vgl. Insecure.org, 2005, 7, <http://www.insecure.org/nmap/versionscan.html>]

- Diverse webbasierte Portscanner erlauben es interessierten Benutzern, ihr System vom Internet aus nach offenen Ports zu scannen. Diese Portscanner sind in ihrer Funktionalität eingeschränkt, jedoch durchaus nützlich, um einen Eindruck zu bekommen, welche Ports eines Systems vom Internet aus geöffnet sind.

### 3.3.2 Schwachstellenscanner

Schwachstellenscanner gehen einen Schritt weiter als Portscanner. Sie identifizieren nicht nur offene Ports, laufende Betriebssysteme und Dienste sowie deren Versionen, sie verbinden diese Information darüber hinaus mit einer Datenbank von Schwachstellen, um direkt Schwachstellen der laufenden Dienste anzuzeigen. Dies ist meist noch mit einer Hilfestellung verbunden, wie die betreffende Schwachstelle zu entfernen ist. Es gibt ebenso wie bei den Portscannern viele verschiedene Schwachstellenscanner, sowohl kommerziell als auch frei verfügbar.<sup>261</sup> Schwachstellenscanner kommen, wie der Name bereits vermuten lässt, bei der Schwachstellenanalyse zum Einsatz, und werden auch bei Penetrationstests häufig eingesetzt.

Die Qualität eines Schwachstellenscanners bestimmt sich aus der Vollständigkeit, Genauigkeit und Umfang der Schwachstellenüberprüfung, sowie aus der Frequenz und Qualität der Updates und der Form der Berichterstellung. Ein letztes Kriterium ist die Preisgestaltung bzw. Lizenzierung.<sup>262</sup>

#### Nessus

Der am weitesten verbreitete Open Source Schwachstellenscanner ist Nessus. Nessus benutzt eine Client-Server Architektur. Ein irgendwo im IT-Netzwerk installierter Nessus-Server lässt sich von Nessus-Clients innerhalb des IT-Netzwerkes zum Scannen des IT-Netzwerkes einsetzen. Durch das strategisch geschickte Platzieren von Nessus-Servern können Scans aus verschiedenen Perspektiven durchgeführt werden.<sup>263</sup> Clients und Server sind für verschiedene Plattformen verfügbar, wobei der Windows-Server kostenpflichtig vertrieben wird. Alles über Nessus ist unter <http://www.nessus.org> zu finden.

Ein weiterer Vorteil von Nessus ist, dass sich externe Programme einbinden lassen, welche die Effektivität des Scans verbessern. Unter anderem kann nmap für die während des Schwachstellenscans benötigten Portscans eingesetzt werden.<sup>264</sup>

---

<sup>261</sup> [Vgl. Anonymous, 2001, S. 276ff]

<sup>262</sup> [Vgl. Anonymous, 2001, S. 280f]

<sup>263</sup> [Vgl. Anderson, Harry (28.10. 2003), Abschnitt 1.0]

<sup>264</sup> [Vgl. Anderson, Harry (28.10. 2003), Abschnitt 2.0]

Nessus benutzt zur Schwachstellenerkennung Plug-Ins, welche in einer eigenen Scriptsprache verfasst sind: NASL (= Nessus Attack Scripting Language). Für jede Schwachstelle, die erkannt werden kann, gibt es ein Plug-In. Das Erstellen neuer Plug-Ins ist einfach möglich und wird durch die hinter dem Nessus-Projekt stehende Gemeinde laufend erledigt. Das Update der Plug-Ins erfolgt über das Internet.<sup>265</sup>

Nessus führt nicht jedes verfügbare Plug-In, welches auf einen durch den Portscan und Version Detection erkannten Dienst anwendbar ist, automatisch aus. Manche können zum Absturz des Systems führen. Diese können vorsichtshalber deaktiviert werden, um den Produktionsprozess nicht zu unterbrechen.<sup>266</sup>

Die Ergebnisse des Schwachstellenscans präsentiert Nessus in Text, als HTML, oder Adobe Acrobat (.pdf) Datei. Der Export der Ergebnisse in verschiedenen Formaten wird ebenfalls unterstützt, darunter ein Format für SQL-Datenbanken.<sup>267</sup>

Nessus ist ein umfassendes und mächtiges Produkt, und seinen kommerziellen „Mitbewerbern“ ebenbürtig und in manchen Aspekten sogar überlegen.<sup>268</sup>

#### **ISS – Internet Scanner**

Der Internet Scanner der Firma Internet Security Systems ist ein Vertreter der kommerziellen Schwachstellenscanner. Vorteile sind die exzellente Berichterstattung, ein umfassender Schwachstellenscan und vor allem die sehr praktische Oberfläche. Der ISS Internet Scanner kann mit Sicherheitsprodukten vernetzt werden, um so auf Basis der Scannerdaten ein Bild der Gefährdung durch IT-Sicherheitslücken zu erstellen.<sup>269</sup> Darüber hinaus bietet der Internet Scanner weitere Funktionen, die das Schwachstellenmanagement einer Organisation standortübergreifend unterstützen.<sup>270</sup> Der Internet Scanner unterstützt lediglich Microsoft Windows Betriebssysteme.<sup>271</sup>

---

<sup>265</sup> [Vgl. Anderson, Harry (28.10. 2003), Abschnitt 3.1]

<sup>266</sup> [Vgl. Anderson, Harry (28.10. 2003), Abschnitt 4]

<sup>267</sup> [Vgl. Anderson, Harry (3.2. 2004), Abschnitt 2]

<sup>268</sup> [Vgl. Anonymous, 2001, S. 285f]

<sup>269</sup> [Vgl. Anonymous, 2001, S. 284]

<sup>270</sup> [Vgl. Internet Security Systems, 2005, 8, InternetScanner\_datasheet.pdf, [http://documents.iss.net/literature/InternetScanner/InternetScanner\\_datasheet.pdf](http://documents.iss.net/literature/InternetScanner/InternetScanner_datasheet.pdf)]

<sup>271</sup> [Vgl. Internet Security Systems, 2005, 8, Internet Scanner Features, [http://www.iss.net/products\\_services/enterprise\\_protection/vulnerability\\_assessment/is\\_requirements.php](http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/is_requirements.php)]

### Weitere Schwachstellenscanner

- GFI LANguard Network Security Scanner der Fa. GFI:  
<http://www.gfi.com/lannetscan/>
- Retina<sup>®</sup> Network Security Scanner der Fa. eEye Digital Security:  
<http://www.eeye.com/html/products/retina/index.html>

### 3.3.3 Datenbankscanner

Auch Datenbanken weisen Sicherheitsschwächen auf. Schwache oder nicht vorhandene Passwörter oder auch nicht benutzte Benutzerkonten sind Beispiele dafür. Datenbankscanner leisten Ähnliches wie Schwachstellenscanner. Der offensichtliche Unterschied ist, dass das Zielsystem eine Datenbank ist. Datenbankscanner sind von verschiedenen Anbietern erhältlich, der bekannteste Vertreter ist der Database Scanner der Fa. ISS, welcher am besten in Verbindung mit dem Internet Scanner eingesetzt wird.

### 3.3.4 Packet Analyzer

Packet Analyzer sind auch gemeinhin als „Sniffer“ bekannt. Sie sind in der Lage, den Netzwerkverkehr aufzuzeichnen und zu analysieren. Verschiedene Protokolle werden erkannt und eine Betrachtung der einzelnen Pakete und gegebenenfalls deren Inhalt ist möglich. Diese Art von Werkzeugen kommt bei einer IT-Sicherheits-Überprüfung nur indirekt zum Einsatz. Schwachstellen in IT-Systemen werden nicht aufgedeckt, jedoch ist eine Analyse des Netzwerkverkehrs zur Vorbereitung eines Penetrationstests sinnvoll, um mögliche Angriffspunkte zu identifizieren oder sogar unverschlüsselt übertragene Passwörter zu entdecken. Jedoch ist anzumerken, dass die Anwendung eines Packet Analyzers im internen Netzwerk nur durch Ausnutzung einer Schwachstelle möglich ist. Das bedeutet zumindest unerlaubten Zugriff auf Switches oder Hubs (und damit Zugang zu Gebäuden und Räumen) bzw. die Erlangung der Kontrolle über einen der Rechner im internen Netz.

Einige bekannte Vertreter der Packet Analyzer sind:

- Etherreal, Open Source, für UNIX, Linux, Mac OS und Microsoft Windows in einer Vielzahl von Portierungen; <http://www.ethereal.com/download.html>
- Ettercap, für folgende Plattformen: Linux 2.x.x, FreeBSD 4.x 5.x, OpenBSD 2.[789] 3.x, NetBSD 1.5, Mac OS X, Microsoft Windows 2000/XP/2003, Solaris 2.x;  
<http://ettercap.sourceforge.net/>

### 3.3.5 Wireless Tools

Drahtlose Netzwerkverbindungen mittels WLAN und auch Bluetooth finden immer weitere Verbreitung. Naturgemäß sind auch drahtlose Verbindungen anfällig gegenüber Angriffen. Drahtlose Verbindungen sind durch ihren Vorteil, ohne Kabelverbindung genutzt werden zu können, dem Nachteil unterworfen, auch von außerhalb des Gebäudes benutzt werden zu können. Für Angriffe auf WLANs (und somit auch für die Überprüfung der Sicherheit von WLANs) stehen einige Werkzeuge zur Verfügung.

#### **Kismet**

Kismet ist ein WLAN Detektor, Sniffer und IDS. Kismet sammelt passiv WLAN Pakete und erkennt so WLANs, selbst wenn sie versteckt sind. Dadurch ist es möglich festzustellen, ob ein WLAN auch noch außerhalb des gewünschten Bereiches verfügbar ist. Durch Einstellung der Signalstärke kann unerwünschter Bereichsabdeckung entgegengewirkt werden. Unzureichend gesicherte Access Points (mit Defaultkonfiguration) werden ebenfalls erkannt. Durch den Einsatz von Kismet können natürlich auch unerwünschte Access Points entdeckt werden. Kismet ist frei erhältlich unter: <http://www.kismetwireless.net/download.shtml>.<sup>272</sup>

#### **Andere Wireless Tools**

Eine Alternative zu Kismet ist Wellenreiter. Wellenreiter ist in der Funktionalität nicht so umfangreich wie Kismet, bietet aber einige spezielle Funktionen, die Kismet nicht besitzt: DHCP und ARP Pakete werden decodiert und dargestellt. Wellenreiter ist ebenfalls frei erhältlich: <http://www.wellenreiter.net/download.html>.<sup>273</sup>

Abgesehen von WLAN Sniffen gibt es noch Werkzeuge, welche die WEP-Verschlüsselung brechen können. Diese sind in der IT-Sicherheits-Überprüfung jedoch nur bedingt von Nutzen und stellen eher Angriffswerkzeuge dar. Eine gebrochene Verschlüsselung kann jedoch von der Notwendigkeit besserer Sicherheitsmaßnahmen überzeugen.

### 3.3.6 Logfile Analyzer

Wie bereits gezeigt, ist es wichtig, die von den IT-Systemen erstellten Protokolle auszuwerten. Dies verlangt jedoch oft einigen Aufwand. Protokolldaten erreichen mit der Zeit großen Um-

---

<sup>272</sup> [Vgl. Kismet, April 2005, 9, Kismet, <http://www.kismetwireless.net/documentation.shtml>]

<sup>273</sup> [Vgl. Wellenreiter, April 2005, 10, Wellenreiter – WaveLAN Hacking, <http://www.wellenreiter.net/index.html>]

fang und sind oft sehr schwierig auszuwerten. Um dieses Problem zu umgehen, stehen Softwarewerkzeuge zur Verfügung, welche die Datenflut bewältigen und das Auswerten erheblich erleichtern. Auch in diesem Bereich der Werkzeuge gibt es viele Vertreter. Die unterschiedlichen Werkzeuge unterstützen verschiedene Protokollformate bzw. verschiedene Systeme.<sup>274</sup>

### LogSurfer

LogSurfer ist ein Logfile-Analyzer, der vom Fachbereich Informatik der Universität Hamburg entwickelt wurde. LogSurfer ist ein mächtiges Werkzeug, welches unverschlüsselte (in Textform vorliegende) Protokolldateien untersucht und auf Basis des Inhalts verschiedene Aktionen ausführen kann. Mögliche Aktionen sind beispielsweise das Erstellen einer Warnmeldung, die Ausführung eines externen Programms oder sogar die Weiterleitung von Teilen des Protokollinhalts an externe Befehle oder Prozesse. LogSurfer ist kostenlos verfügbar unter <ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/>.<sup>275</sup>

### Weitere Logfile-Analyzer

- WebTrends Webanalyse der Fa. WebTrends Corp. ist ein Werkzeug zur Analyse der Webserveraktivität, und stellt eine mächtige Lösung mit umfassenden Reportingfähigkeiten dar. <http://www.webtrends.com>
- Sane Solutions LLC bietet eine Produktpalette unter dem Namen NetTracker, welche in der Lage ist, die Aktivitäten von Firewalls, Proxies, FTP-Servern und Webservern zu analysieren und darzustellen. <http://www.sane.com/>

### 3.3.7 Werkzeugsammlungen

Zur Durchführung von IT-Sicherheits-Überprüfungen geeignete Werkzeuge werden oftmals in Werkzeugsammlungen zusammengefasst, um den Zugriff auf die einzelnen Werkzeuge zu erleichtern. Anstatt alle Werkzeuge einzeln zu beschaffen, sind alle nötigen Werkzeugklassen, oft sogar verschiedene ihrer Vertreter, auf einem Medium vereint. Ein Beispiel für diese Art von Werkzeugsammlung ist die Auditor Security Collection.

### Auditor

Auditor ist eine Plattform für Penetrationstests. Direkt von der CD gestartet, kommt Auditor ohne jegliche Installation aus. Die Hardware des benutzten Rechners wird automatisch erkannt und ein Linuxsystem wird gestartet, welches eine umfangreiche Sammlung von ca. 300

---

<sup>274</sup> [Vgl. Anonymous, 2001, S. 313f]

<sup>275</sup> [Vgl. Anonymous, 2001, S. 314]

Open Source Softwarewerkzeugen bereitstellt. Diese sind in einer Menüstruktur nach den Phasen eines Penetrationstests angeordnet. Dies erleichtert die Auswahl des gewünschten Werkzeugs. Zusätzliche Hilfsmittel sind ebenfalls inkludiert, beispielsweise Wörterbücher um Passwörter zu knacken oder Hintergrundinformationen über Standardkonfigurationen und – passwörter. Abgerundet wird Auditor durch eine Reihe von Programmen, welche zum Erstellen von Texten und Berichten geeignet sind, sowie durch Standardapplikationen wie Webbrowser oder Graphikeditoren.<sup>276</sup>

Auditor ist sehr nützlich, um schnelle, punktuelle Überprüfungen selbst vorzunehmen. Ein professioneller Penetrationstester wünscht sich allerdings eine besser auf seine Vorlieben anpassbare Umgebung.

#### **3.3.8 Unterstützende Werkzeuge für umfassende Methodiken**

Für die Umsetzung der umfassenden Methodiken, welche in Kapitel 2 der vorliegenden Arbeit beschrieben wurden, stehen ebenfalls einige Werkzeuge zur Verfügung. Einige Vertreter wurden bereits in Abschnitt 2.5.2 erwähnt. Eines dieser Werkzeuge soll im Folgenden stellvertretend für die anderen beschrieben werden: Das BSI Grundschutz-Tool.

##### **BSI Grundschutz-Tool**

Das BSI Grundschutz-Tool erleichtert die Anwendung des BSI GS HB. Aufbauend auf einem aktuellen, komplexitätsreduzierten Netzwerktopologieplan werden die Zielobjekte strukturiert. Darunter wird die Verknüpfung von Gebäuden, Räumen, IT-Systemen und Applikationen verstanden. Die Strukturierung wird graphisch in einer hierarchischen Baumstruktur angezeigt. Die größte Erleichterung bei der Anwendung des GS HB erfolgt bei der Modellierung des IT-Verbundes. Anwendbare Bausteine (Gefährdungs- und Maßnahmenkataloge) werden den Zielobjekten automatisch zugeordnet. Dazu muss zuvor bei der Erfassung der Typ des erfassten Objektes eingetragen werden. Auch die Einbindung von eigenen Gefährdungs- und Maßnahmenkatalogen ist möglich.<sup>277</sup>

Ist die Strukturierung und Modellierung abgeschlossen, kann mit dem Basis-Sicherheitscheck begonnen werden. Bei jedem Objekt sind die ihm zugeordneten Maßnahmen angezeigt und können in ihrem Umsetzungsstatus („ja“, „nein“, „teilweise“ und „entbehrlich“) verändert

---

<sup>276</sup> [Vgl. Remote Exploit, Mai 2005, 11, Auditor main – Rexploit, [http://new.remote-exploit.org/index.php/Auditor\\_main](http://new.remote-exploit.org/index.php/Auditor_main)]

werden. Die beiden letzten Kategorien müssen, um sie anzuwenden, mit einer Begründung versehen werden, um eine leichtfertige Anwendung zu verhindern.<sup>278</sup>

Abgesehen von der graphischen Darstellung des Umsetzungsstatus durch farbige Symbole bei jeder Maßnahme erleichtert das Grundschutz-Tool den Umgang mit den Zertifizierungsstufen des BSI Grundschutzansatzes, indem für die Zertifizierung bzw. die Vorstufen der Zertifizierung nötige Maßnahmen markiert werden.<sup>279</sup>

Neben der Vereinfachung der Strukturierung und Modellierung des IT-Verbundes liegt der große Vorteil des Grundschutz-Tools in der automatisierten Berichterstellung. Die Auswahl von Zielobjekten erlaubt die Erstellung von Berichten, welche sich nur auf Teile des IT-Verbundes beziehen. Berichte werden im HTML-Format generiert, und können so bearbeitet und etwa an die Corporate Identity der Organisation angepasst werden.<sup>280</sup>

Das BSI Grundschutz-Tool stellt eine echte Erleichterung für Anwender des GSHB dar, hat jedoch auch ein paar Schwächen. Zum einen ist das Grundschutz-Tool nicht kompatibel mit Netzwerkmanagementsystemen, was die Datenhaltung teilweise redundant werden lässt, da die Struktur des IT-Verbundes nicht importiert werden kann. Zum anderen ist das Grundschutz-Tool plattformabhängig entwickelt. Eine Webanwendung wäre sinnvoller, um das Grundschutz-Tool nicht auf allen Rechnern, auf denen es zum Einsatz kommen soll, installieren zu müssen.<sup>281</sup>

---

<sup>277</sup> [Vgl. Scheiderer, 2004, S. 57f]

<sup>278</sup> [Vgl. Scheiderer, 2004, S. 58]

<sup>279</sup> [Vgl. Scheiderer, 2004, S. 58f]

<sup>280</sup> [Vgl. Scheiderer, 2004, S. 59]

<sup>281</sup> [Vgl. Scheiderer, 2004, S. 59]

## 4 IT-Sicherheits-Überprüfungen als Dienstleistungen

Viele Unternehmen wollen oder können aus verschiedenen Gründen IT-Sicherheits-Überprüfungen ihrer IT-Infrastruktur nicht selbst durchführen. Ein Grund dafür ist das zur Durchführung einer IT-Sicherheits-Überprüfung nötige Fachwissen, welches nicht in jedem Unternehmen vorhanden ist. Ausgebildete Fachkräfte sind nötig. Die feste Anstellung von ausgebildetem Fachpersonal ist jedoch teuer. Diesen Kostenaufwand wollen viele Unternehmen nicht aufbringen. Ein weiterer Grund ist der für eine umfassende IT-Sicherheits-Überprüfung nötige Zeitaufwand.

IT-Sicherheits-Überprüfungen werden von vielen Unternehmen in Österreich als Dienstleistungen angeboten. Die Angebote bilden ein breites Spektrum und eignen sich für unterschiedliche Zielsetzungen. Ein Ziel dieser Arbeit ist es, zu untersuchen, wie die Methoden und Werkzeuge der IT-Sicherheits-Überprüfungen in Österreich angeboten werden.

### 4.1 Fragebogen zur Klärung des Dienstleistungsangebots

Um das Angebot der IT-Sicherheits-Überprüfungen in Österreich zu untersuchen, kam ein Fragebogen zum Einsatz, der an eine Auswahl von Unternehmen unterschiedlicher Größen verschickt wurde. Der komplette Fragebogen ist in Anhang H der vorliegenden Arbeit zu finden. Der Fragebogen wurde gestaltet, um zu ergründen, inwiefern die betreffende Dienstleistung im Rahmen einer IT-Sicherheits-Überprüfung einsetzbar ist, respektive wie umfassend die Dienstleistung gestaltet ist. Anhand der erhaltenen Antworten wird in der Folge versucht, die Marktsituation für IT-Sicherheits-Überprüfungen einzuschätzen und zu bewerten.

Der Fragebogen klärt ab, ob das befragte Unternehmen IT-Sicherheits-Überprüfung in ihrem Kerngeschäft durchführt, und für welche Kunden das Angebot zugeschnitten ist. Die möglichen Kunden werden in drei Kategorien eingeteilt: Klein- und mittelständische Unternehmen, große Unternehmen bzw. Konzerne, und Unternehmen mit speziellem Sicherheitsbedarf.

Anschließend wird untersucht, ob und auf welche IT-Infrastrukturen, Applikationen und IT-Systeme das Angebot beschränkt ist. Daran werden eventuelle Spezialisierungen der Unternehmen sichtbar.

Der nächste Abschnitt des Fragebogens befasst sich mit der Art der IT-Sicherheits-Überprüfung. Benutzte Methoden, überprüfte Aspekte der IT-Sicherheit und die dabei eingesetzten Werkzeuge sind anzuführen.

Abschließend erfasst der Fragebogen eventuelle Preisgestaltungen und zusätzliche Leistungen des Angebots, wie etwa Verbesserungsvorschläge und Hilfestellungen bei der Implementierung.

### **4.2 Klassifizierung des Angebots**

Um das Angebot der IT-Sicherheits-Überprüfungen in Österreich zu klassifizieren, erfolgt zuerst die Betrachtung der von den befragten Unternehmen retournierten Fragebögen. Dabei wird nach Dienstleistungsunternehmen unterschieden, welche die IT-Sicherheits-Überprüfung zu ihrem Kerngeschäft zählen und welche dies nicht tun. Beide Varianten sind in Österreich verbreitet.

Anschließend werden einige Dienstleistungen erläutert, welche in Österreich angeboten werden, jedoch nicht in die Umfrage miteinbezogen wurden, da sie Spezialfälle innerhalb des Marktes darstellen.

### **IT-Sicherheits-Überprüfungen außerhalb des Kerngeschäfts**

Jene Unternehmen, welche IT-Sicherheits-Überprüfungen außerhalb ihres Kerngeschäftes anbieten, richten ihr Angebot hauptsächlich an klein- und mittelständische Unternehmen. Ein kleiner Teil zählt auch größere Unternehmen und Unternehmen mit speziellem Sicherheitsbedarf zu ihrem Kundenkreis, dies jedoch wohl aufgrund ihrer Tätigkeiten als Internet Service Provider (=ISP). Dies lässt vermuten, dass die Durchführung von IT-Sicherheits-Überprüfungen eine begleitende Dienstleistung an bestehende Kunden ist, welche den betreffenden ISP-Service in Anspruch nehmen.

Beschränkungen auf etwaige IT-Infrastrukturen kommen in verschiedener Ausprägung vor, zu allererst ist hierbei wieder die Beschränkung auf WAN-Infrastrukturen bzw. DMZ bei ISPs zu erwähnen. Andere Beschränkungen sind weit gestreut. Ein Anbieter bietet IT-Sicherheits-Überprüfungen der Telekommunikationsanlagen an. Auch die Überprüfung von VoIP-Infrastrukturen wird von einem der befragten Dienstleistungsunternehmen angeboten. Auffallend ist die häufig fehlende Überprüfung der WLAN-Infrastrukturen. Durchgehend werden lediglich IT-Sicherheits-Überprüfungen der LAN-Infrastruktur angeboten.

Auffallend ist, dass keines der befragten Unternehmen sich bei der IT-Sicherheits-Überprüfung auf spezielle IT-Systeme oder Applikationen beschränkt. Somit sollten diese Anbieter in der Lage sein, auch exotische Plattformen auf ihre IT-Sicherheit zu prüfen, sowie

ein beträchtliches Fachwissen in ihrem Unternehmen konzentrieren. Im Vergleich zu den Dienstleistungsunternehmen, welche IT-Sicherheits-Überprüfungen in ihrem Kerngeschäft anbieten, fällt auf, dass diese sich sehr wohl auf bestimmte IT-Systeme und Applikationen beschränken. Daraus lässt sich schließen, dass die fehlende Einschränkung zumindest teilweise auf fehlende Fachkompetenz bzw. Vollständigkeit der IT-Sicherheits-Überprüfung zurückzuführen ist.

Die von den Dienstleistungsunternehmen angewandten Methoden zur IT-Sicherheits-Überprüfung sind von Fall zu Fall sehr unterschiedlich. Nur zwei der befragten Unternehmen decken sowohl interne als auch externe Tests sowie die Sichtung von Konfigurationen und IT-Sicherheitspolitiken ab. Dementsprechend ist in diesem Fall keine einfache Aussage über die Qualität des Dienstleistungsangebots zu machen. Vielmehr ist es nötig, die Dienstleistungen gezielt nach dem eigenen Bedürfnis auszuwählen. Eine umfassende Überprüfung mittels Penetrationsversuchen und Prüfung der organisatorischen Sicherheit ist allerdings nicht zu erwarten.

Diese Einschätzung wird durch die Auswertung der überprüften Aspekte der IT-Sicherheit bestätigt. Kein einziges der befragten Unternehmen deckt sämtliche Aspekte ab, das vollständigste der Angebote lässt lediglich die Überprüfung der Gebäudesicherheit außen vor. ISPs beschränken sich auf die Überprüfung der eigenen aktiven Komponenten und stellen so wiederum einen Sonderfall dar.

Bei der IT-Sicherheits-Überprüfung kommen sowohl kommerzielle als auch frei erhältliche Software-Werkzeuge zum Einsatz. Einige Unternehmen verwenden beide Varianten, andere verlassen sich ausschließlich auf freie Werkzeuge. Keines der befragten Unternehmen gab an, ausschließlich kommerzielle Werkzeuge zu benutzen. Ein Ergebnis, welches aufgrund der hohen Qualität der verfügbaren freien Werkzeuge nicht überrascht.

Der Großteil der befragten Unternehmen liefert nach der Überprüfung Vorschläge zur Verbesserung der IT-Sicherheit, Hilfe bei deren Implementierung jedoch lediglich gegen Aufpreis. In beide Richtungen gibt es jedoch Ausnahmen, ein Anbieter verlangt für Verbesserungsvorschläge bereits einen Aufpreis, bei einem anderen ist die Implementierungshilfe eine Inklusivleistung.

Abbildung 4-1 veranschaulicht die Vollständigkeit des Angebotes und die dazugehörigen Zielgruppen. Jeder rote Balken stellt ein Angebot dar, welches als Antwort auf einen Frage-

bogen einging. Die Vollständigkeit berechnet sich aus der Summe der in Frage 8 und 9 angekreuzten Punkte (maximal 16), plus eventueller Bonuspunkte für die Orientierung an standardisierten Methodiken. Der Kundenkreis ist direkt aus Frage 2 ablesbar.



**Abbildung 4-1: Angebotsklassifizierung für Angebote außerhalb des Kerngeschäftes**

Quelle: Autor

### IT-Sicherheits-Überprüfungen im Kerngeschäft

Werden IT-Sicherheits-Überprüfungen innerhalb des Kerngeschäfts angeboten, richten sich die Angebote in größerem Ausmaß auch an größere Unternehmen und Unternehmen mit besonderem Sicherheitsbedarf. Lediglich ein befragtes Unternehmen beschränkt sich auf klein- und mittelständische Unternehmen als Kunden. Ebenso schließt nur ein befragtes Dienstleistungsunternehmen Unternehmen mit erhöhtem IT-Sicherheitsbedarf als Kunden aus. Der Rest der Dienstleistungsunternehmen ist allen Unternehmensgrößen gegenüber aufgeschlossen.

IT-Infrastrukturen werden von keinem Dienstleistungsunternehmen ausgeschlossen. Durch über den Fragebogen hinausgehende Zusatzinformationen der befragten Unternehmen ist ersichtlich, dass sich das betreffende Angebot auf alle Bereiche der IT-Sicherheit erstreckt,

bzw. der ISO/IEC 17799 folgt und den IT-Sicherheitsmanagement-Prozess gesamtheitlich betrachtet.

Beschränkungen des Dienstleistungsangebots auf bestimmte IT-Systeme kommen vor, wie etwa Beschränkungen auf Microsoft Windows und Linux. Von den IT-Systemen unabhängige Angebote sind jedoch weit verbreitet, viele Betriebssysteme und Firewalls sind in den Angeboten eingeschlossen.

Der Großteil der Angebote beschränkt sich nicht auf spezielle Applikationen, einige Unternehmen gaben bei der Beantwortung der Fragebögen eine Auswahl der Applikationen an, wie etwa bestimmte Datenbanken oder Webserver. Andererseits werden Applikationen nicht in jedem Angebot im Detail betrachtet.

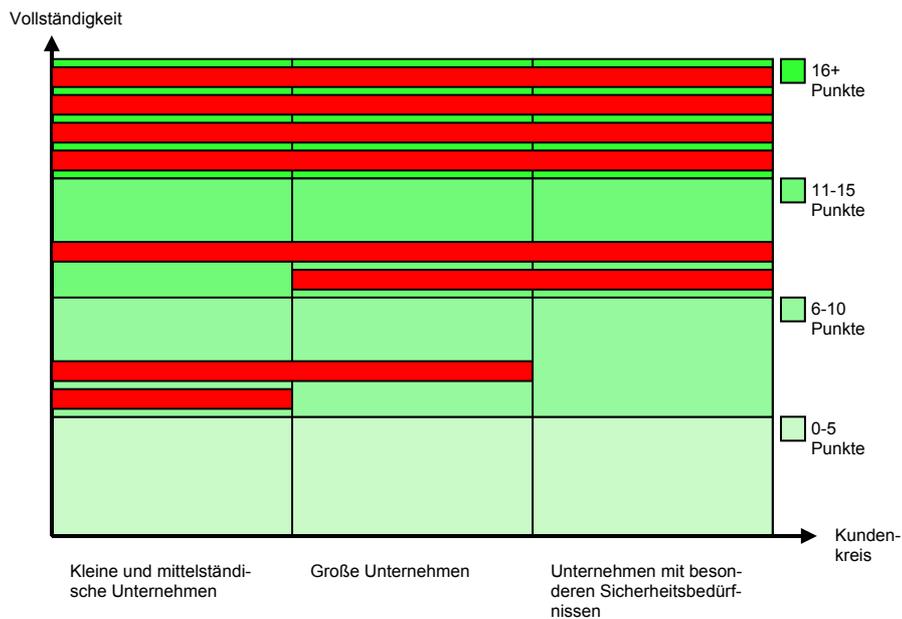
Bei der Betrachtung der von den Dienstleistungsunternehmen angewandten Methoden fällt auf, dass sämtliche Methoden auch angewandt werden. Lediglich zwei Anbieter verzichten (teilweise aus ethischen Gründen) auf gezielte Angriffsversuche.

Die überprüften Aspekte sind im Vergleich zu den Unternehmen, welche IT-Sicherheits-Überprüfungen außerhalb des Kerngeschäfts anbieten, vollständig. Viele Unternehmen überprüfen sämtliche Aspekte. Insgesamt gesehen sind Defizite wiederum bei der Gebäudesicherheit sowie der Überprüfung der verantwortlichen Personen vorhanden.

Beim Einsatz von Softwarewerkzeugen verwenden fast alle befragten Unternehmen sowohl freie als auch kommerzielle Varianten. Lediglich ein Unternehmen benutzt ausschließlich frei verfügbare Werkzeuge bei ihren IT-Sicherheits-Überprüfungen.

Alle befragten Unternehmen bieten Vorschläge für die Verbesserung der IT-Sicherheit ohne Aufpreis an. Implementierungshilfen dieser Verbesserungsvorschläge werden gegen Aufpreis beziehungsweise durch Folgeaufträge angeboten.

Abbildung 4-2 veranschaulicht die Vollständigkeit der Angebote jener Unternehmen, welche IT-Sicherheits-Überprüfungen in ihrem Kerngeschäft anbieten.



**Abbildung 4-2: Angebotsklassifizierung für Angebote innerhalb des Kerngeschäftes**

Quelle: Autor

### Spezielle Dienstleistungen

Das Angebot an Dienstleistungen im Bereich der IT-Sicherheits-Überprüfungen wird durch einige spezielle Angebote ergänzt. Zum einen ist es für eine Organisation möglich, ihren IT-Sicherheitsmanagement-Prozess nach ISO/IEC 17799 zertifizieren zu lassen. Zum anderen stellen Ziviltechniker öffentlich anerkannte Urkunden und technische Gutachten aus.

Ein Unternehmen in Österreich bietet Zertifizierungen nach ISO/IEC 17799 bzw. BS 7799 an. Dies bietet Organisationen die Möglichkeit, ihren IT-Sicherheitsmanagement-Prozess nach der international anerkannten ISO-Norm bestätigen zu lassen. Das Zertifikat wird nach einem mehrstufigen Prozess, der Vorbeurteilung und Hilfestellungen durch Feststellung von Mängeln und Verbesserungspotenziale beinhaltet, für drei Jahre ausgestellt. Danach folgt jährlich eine Überprüfung auf Effektivität des IT-Sicherheitsmanagement-Prozesses und dessen ständige Verbesserung. Nach Ablauf der Gültigkeit kann das Zertifikat erneuert werden.

Ziviltechniker sind in Österreich für die Notariatskammer tätig und stellen offizielle, staatlich anerkannte Prüfungsberichte, Urkunden und technische Gutachten unter anderem auch im Bereich der IT-Sicherheit aus. Dies bietet für Organisationen die Möglichkeit, ihre Bestre-

bungen im Bereich der IT-Sicherheit offiziell bestätigen zu lassen. Dies ist natürlich hilfreich, um gegenüber den Kunden bzw. Geschäftspartnern eine offizielle Beurkundung vorweisen zu können.

### 4.2.1 Stärken

Zusammenfassend lässt sich feststellen, dass das Angebot an Dienstleistungen für IT-Sicherheits-Überprüfungen in Österreich Stärken bei gezieltem Outsourcing besitzt. Einige Dienstleistungen eignen sich, um die bei einer organisationsinternen Anwendung eventuell fehlenden Ressourcen auszugleichen; beispielsweise bei der Durchführung der Schwachstellenanalyse bei der OCTAVE<sup>SM</sup>-Methodik. Einige wenige Angebote bieten aber auch umfassende Überprüfungen des IT-Sicherheitsmanagement-Prozesses gemäß ISO/IEC 17799 oder eine Methodik, welche auf dem BSI-Grundschutzansatz aufbaut.

Zertifizierungen nach ISO/IEC sowie die behördlichen Status genießenden Urkunden der Ziviltechniker sind ebenfalls sinnvolle Dienstleistungen.

### 4.2.2 Schwächen

Die grundlegende Schwäche des österreichischen Dienstleistungsangebotes im Bereich der IT-Sicherheits-Überprüfung ist, dass es sich wenig für umfassende IT-Sicherheits-Überprüfungen eignet. Die Angebote sind in den meisten Fällen unvollständig und erfüllen kein hohes Sicherheitsniveau. So ist es bei ihrer Inanspruchnahme nötig, sich über die Defizite im Klaren zu sein. Das zugrunde liegende Bild ist eine fehlende Standardisierung der Dienstleistungen.

## 4.3 Problematik der nichtstandardisierten Dienstleistung

Grundsätzlich fällt bei der Bearbeitung der Umfrageergebnisse auf, dass die Dienstleistungen äußerst unterschiedlich ausfallen, und sich bis auf wenige Ausnahmen nicht an standardisierten Methodiken zur Überprüfung der IT-Sicherheit (OCTAVE, BSI Grundschutz, COBIT) orientieren. Stattdessen kommen selbst entwickelte Methodiken zum Einsatz, jedes Unternehmen schneidert sich ein Angebot zusammen und entwickelt ein mehr oder weniger ausgereiftes Überprüfungskonzept. Einzelne Angebote orientieren sich an etablierten Vorgangsweisen (Penetrationstest), diese bilden jedoch eher die Ausnahme. Abgesehen davon stellt sich das Angebot sehr uneinheitlich dar, viele Unternehmen bieten IT-Sicherheits-Überprüfungen außerhalb ihres Kerngeschäftes an. Einige davon erwecken den Eindruck,

keinem sehr hohen IT-Sicherheitsstandard zu entsprechen. Diese Angebote richten sich allerdings auch eher an kleine und mittelständische Unternehmen. Diejenigen Anbieter, welche die Überprüfung der IT-Sicherheit zu ihrem Kerngeschäft zählen, bieten auch durchwegs höhere Standards, und zählen auch Unternehmen mit erhöhtem Sicherheitsbedarf zu ihren Kunden.

Der Schwerpunkt der Angebote liegt in der Überprüfung der technischen Sicherheit, und nähert sich einem Penetrationstest an. Jedoch bleibt meist – auch bei Anbietern mit höherer Professionalität - zumindest ein Aspekt der IT-Sicherheit unbeachtet. In den meisten Fällen wird die Gebäudesicherheit (Zugangskontrollen) vernachlässigt. Eine zweite Nachlässigkeit ist die Überprüfung der Durchsetzung der IT-Sicherheits-Politiken durch das verantwortliche Personal.

Doch das Angebot in Österreich hat nicht nur Schattenseiten. Einzelne Anbieter bieten IT-Sicherheits-Überprüfungen nach internationalen Standards (ISO/IEC 17799) bzw. IT-Sicherheits-Überprüfungen, welche auf der Basis des Standards selbst entwickelt wurden. Durch einen Anbieter ist die Zertifizierung nach ISO/IEC 17799 möglich. Ziviltechniker bieten Zertifizierungen der IT-Sicherheit, die offiziell und amtlich anerkannt sind.

Positiv ist zu bemerken, dass beinahe alle befragten Unternehmen nach ihrer IT-Sicherheits-Überprüfung Vorschläge zur Verbesserung der IT-Sicherheit bieten, und auch Unterstützung bei der Umsetzung derselben anbieten.

Bei der Betrachtung der Dienstleistungen im Bereich der IT-Sicherheits-Überprüfungen in Österreich ist erkennbar, dass es viele Anbieter gibt, jedoch nur wenige Spezialisten in der Lage sind, die IT-Sicherheit auf umfassende Weise zu überprüfen. Im Gegensatz dazu bieten sich die anderen Angebote eher dazu an, punktuelle IT-Sicherheits-Überprüfungen durchzuführen, die ein unternehmenseigenes Projekt unterstützen können.

## 5 Resumee

Die IT-Sicherheit sicherzustellen, ist für eine Organisation in der heutigen Zeit enorm wichtig. Bedrohungen, die daraus entstehenden Risiken und deren Kosten, sowie gesetzliche und auch vertragliche Vorgaben zwingen jede Organisation, welche informationsverarbeitende Systeme einsetzt, diese auch entsprechend zu sichern. Leider wird auch heutzutage immer noch der Fehler gemacht, sich allein auf die technische IT-Sicherheit zu konzentrieren, und die Managementabläufe außer Acht zu lassen. Um eine umfassende IT-Sicherheit zu erreichen, ist ein IT-Sicherheitsmanagement-Prozess notwendig. Eine effiziente Methodik um einen IT-Sicherheitsmanagement-Prozess zu etablieren und schnell ein relativ hohes Maß an IT-Sicherheit zu erreichen, ist der BSI-Grundsatzansatz.

Der IT-Sicherheitsmanagement-Prozess ist ein fortlaufender Prozess, welcher sich selbst verbessert und einen Lebenszyklus bildet. Nur durch die sich ständig wiederholenden Abläufe, und die darin enthaltene Selbstverbesserung kann die IT-Sicherheit gewährleistet werden. Bestandteil des IT-Sicherheitsmanagement-Prozesses sind Überprüfungen der IT-Sicherheit, welche Mängel aufdeckt, die im Fortlauf des Zyklus behoben werden. Die Notwendigkeit der IT-Sicherheits-Überprüfung geht direkt aus dem IT-Sicherheitsmanagement-Prozess hervor.

Es gibt viele Methodiken und Techniken, um die IT-Sicherheit zu überprüfen. Die Frage nach einer idealen Methodik lässt sich nicht umfassend beantworten. Zu groß sind die Unterschiede zwischen den einzelnen Organisationen und den von ihnen eingesetzten IT-Infrastrukturen. Jede Organisation muss sich bei einer geplanten Durchführung einer IT-Sicherheits-Überprüfung Gedanken über die für sie richtige Methodik machen. Unbedingt notwendig ist es jedoch, eine IT-Sicherheits-Überprüfung zu finden, welche den gesamten IT-Sicherheitsmanagement-Prozess betrachtet, und sich nicht auf Teilsaspekte beschränkt. Zu groß ist sonst die Gefahr, sich wiederum nur auf die technische IT-Sicherheit zu konzentrieren und eine einseitige IT-Sicherheits-Überprüfung durchzuführen. Die Gefahren hinter einseitigen IT-Sicherheits-Überprüfungen sind fehlender Schutz, sowie ein falsches Sicherheitsbewusstsein in der Organisation.

Die in dieser Arbeit vorgestellten Methodiken zur IT-Sicherheits-Überprüfung sind sehr unterschiedlich. Verschiedene Organisationen werden in verschiedenen Situationen jeweils eine andere Methodik bevorzugen.

Die BSI-Grundschutzmethodik liefert das nötige Werkzeug, um in einer Organisation schnell und möglichst einfach ein angemessenes IT-Sicherheitsniveau zu etablieren. Sie bietet sich für Organisationen an, welche auf eine umfassende Risikoanalyse verzichten wollen. Bei der Überprüfung der IT-Sicherheit hat die BSI-Grundschutzmethodik den Nachteil, dass sie lediglich die Grundschutzbausteine auf ihre Anwendung überprüft. Ergänzende Maßnahmen, welche oft nötig sind, werden nicht im Soll-Ist-Vergleich betrachtet. So wird oft eine ergänzende Sicherheitsanalyse nötig.

Ein wirklich umfassender und empfehlenswerter Ansatz ist der OCTAVE<sup>SM</sup>-Ansatz. Aus ihm geht die OCTAVE<sup>SM</sup>-Methodik hervor. Diese hat den Vorteil, dass sie eine umfassende, das IT-Sicherheitsmanagement miteinbeziehende Bewertung beinhaltet und durch die Organisation selbstgesteuert ist. Nicht vorhandenes Know-How kann jedoch dennoch von außerhalb der Organisation hinzugezogen werden, falls es die Situation erfordert. OCTAVE<sup>SM</sup> bewertet Risiken in Bezug auf kritische Unternehmenswerte, und beleuchtet das Thema der IT-Sicherheit aus der Sicht der Organisationsziele und -politik. OCTAVE<sup>SM</sup> ist eine empfehlenswerte Methodik für Unternehmen, welche durchaus gewillt sind, einiges an Zeit und Arbeitsaufwand in die IT-Sicherheit zu investieren. Der vergleichsweise hohe Aufwand ist allerdings gerechtfertigt, da die OCTAVE<sup>SM</sup>-Methodik konkrete Maßnahmen zur Verbesserung der IT-Sicherheit liefert, und umfassend ausgerichtet ist.

Ist eine Zertifizierung für die Organisation wichtig, ist die BSI-Grundschutzmethodik empfehlenswert. Sie ist als Quasistandard weit verbreitet und zeichnet sich durch eine gute Zertifizierbarkeit aus.

COBIT ist zur eigenen Durchführung weniger geeignet als die anderen in dieser Arbeit vorgestellten Methodiken. COBIT wird hingegen von Wirtschaftsprüfungsunternehmen gerne zur Bewertung der IT-Control in Unternehmen eingesetzt.

Bei IT-Sicherheits-Überprüfungen kommen viele verschiedene Methoden und Werkzeuge zum Einsatz. Eine genaue Auflistung aller Werkzeuge war im Rahmen der vorliegenden Arbeit gar nicht möglich. Bei den Hilfsmitteln (Werkzeugen und Checklisten) wird ein Gegensatz deutlich, der sich durch die ganze Thematik der IT-Sicherheits-Überprüfungen zieht: die technische Sicherheit und das IT-Sicherheitsmanagement (organisatorische Sicherheit). Beides muss geprüft werden, um einseitige IT-Sicherheits-Überprüfungen zu verhindern. Ein ganzes Arsenal an Softwarewerkzeugen hilft bei der Überprüfung der technischen Sicherheit. Check-

listen werden von den Entwicklern verschiedener Methodiken oder Spezialisten der IT-Sicherheit ebenfalls in großer Anzahl veröffentlicht.

Um sicherzustellen, dass die IT-Sicherheits-Überprüfung nicht einseitig ist, bieten sich zwei Optionen an: Einerseits die Anstellung von externen Spezialisten, welche umfassend arbeiten; andererseits die Anwendung einer umfassenden, selbstgesteuerten Methodik durch die Organisation selbst.

Möchte eine Organisation in Österreich ein Outsourcing der IT-Sicherheits-Überprüfung vornehmen, ist das Dienstleistungsangebot von direkter Relevanz. Bei der Durchführung von umfassenden Methodiken durch die Organisation selbst kann es jedoch ebenfalls zu Situationen kommen, in denen externe Dienstleistungen in Anspruch genommen werden. Dies ist sinnvoll, um fehlendes Know-How in der Organisation auszugleichen.

Verschiedene Dienstleistungsangebote können verschiedene Bedürfnisse befriedigen. Umfassende Dienstleistungen sind für ein komplettes Outsourcing nötig, punktuelle Dienstleistungen können beim gezielten Outsourcing eingesetzt werden. Um festzustellen, welche Dienstleistungen in Österreich angeboten werden, kam ein Fragebogen zum Einsatz. Am Ergebnis der Umfrage war erkennbar, dass in Österreich das Angebot an punktuellen, sich auf die technische IT-Sicherheit konzentrierenden Dienstleistungen vorherrscht. Nur wenige Anbieter sind in der Lage, die IT-Sicherheit umfassend zu überprüfen.

Zusätzliche Dienstleistungen sind nötig, um die IT-Sicherheit einer Organisation zu zertifizieren oder urkundlich zu bestätigen. In Österreich gibt es lediglich einen Anbieter, welcher Zertifizierungen nach ISO/IEC 17799 durchführt. Urkunden, welche behördlichen Status genießen, werden von Ziviltechnikern ausgestellt.

Der Markt für IT-Sicherheits-Überprüfungen in Österreich ist also wenig entwickelt. Punktuelle Dienstleistungen herrschen vor, nur wenige Anbieter bieten umfassende IT-Sicherheits-Überprüfungen an. Überprüfungen nach umfassenden Methodiken werden kaum durchgeführt. Der Umstand, dass nur ein Anbieter Zertifizierungen nach ISO/IEC 17799 durchführt, ist ebenfalls ein großer Mangel. Organisationen haben somit nicht die Möglichkeit, aus mehreren Anbietern auszuwählen. Durch steigende Nachfrage, welche zweifelsfrei in der Zukunft entstehen wird, ist zu erwarten, dass auch das Potential des österreichischen Marktes für IT-Sicherheits-Überprüfungen weiter entwickelt werden wird. Damit sollten sich die Defizite langsam ausgleichen.

## **Glossar**

### **Analyseteam**

Das Analyseteam ist für die Durchführung der OCTAVE<sup>SM</sup>-Methode verantwortlich.

### **Area of Concern**

Eine Area of Concern ist ein Bereich der Organisation, welcher durch das Personal im Bezug auf die IT-Sicherheit als interessant bzw. bedroht eingestuft wird. Die Area of Concern wird durch das spezielle Wissen des Personals über die Abläufe in der Organisation für die IT-Sicherheits-Überprüfung interessant.

### **Audit**

Unter Audit wird eine Überprüfung der IT-Control bzw. IT-Sicherheit verstanden, welche vor Ort und von ausgebildetem Personal durchgeführt wird.

### **Bedrohungsbaum**

Der Bedrohungsbaum dient zur Darstellung von Bedrohungsprofilen.

### **Bedrohungsprofil**

Das Bedrohungsprofil ist eine strukturierte Art, die Bedrohungen auf einen Unternehmenswert darzustellen.

### **BSI**

Bundesamt für Sicherheit in der Informationstechnik

### **Business Requirements for Information**

Als Business Requirements for Information werden in der COBIT-Methodik jene Anforderungen an die Informationen bezeichnet, die nötig sind, um die Organisationsziele zu erreichen. Sie entstehen durch die Zusammenfassung von Referenzmodellen und die Entfernung von Redundanzen.

**Catalog of Practices**

→ Maßnahmenkatalog

**CERT**

Computer Emergency Response Team; befasst sich mit den Ursachen, Auswirkungen, Aufzeichnung und Auswertung von Incidents und liefert Hilfestellungen bei der Behandlung von Incidents

**CERT®/CC**

Das CERT® Coordination Center der Carnegie Mellon University ist das erste Computer Security Incident Response Team weltweit. Das CERT®/CC bietet umfassende Statistiken die Computersicherheit betreffend.

<http://www.cert.org>

**Change Management**

Aktivitäten, welche als Reaktion auf Änderungen im IT-System durchgeführt werden, um das erreichte IT-Sicherheitsniveau zu erhalten bzw. zu steigern

**CobIT**

Control Objectives for Information and related Technology; Standard für gute IT-Sicherheit und Kontrollmaßnahmen, welcher von IT Governance Institute herausgegeben wird

**Compliance**

Compliance bezeichnet die Übereinstimmung von Maßnahmen mit den Strategien und Plänen des IT-Managements.

**Control**

Control ist die Summe der Politiken, Prozeduren, Praktiken und organisatorischen Strukturen, welche so gestaltet sind, dass Organisationsziele erreicht und unerwünschte Ereignisse verhindert oder erkannt und korrigiert werden.

**Critical Success Factors**

Die Critical Success Factors bestimmen die wichtigsten Maßnahmen, die durch das Management getroffen werden müssen, um die IT-Control sicherzustellen.

**CSFs**

→Critical Success Factors

**Demilitarisierte Zone**

Zone des Netzwerkes, welche aus dem externen Netz erreichbar, aus Gründen der IT-Sicherheit jedoch vom internen Netz getrennt ist.

**Disaster Recovery**

Vorgang der Wiederaufnahme des Betriebes nach einem Systemausfall

**DMZ**

→Demilitarisierte Zone

**DSG**

Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idF. BGBl. I Nr. 136/2001

**GSHB**

Grundschutzhandbuch des BSI

**IDS**

Intrusion Detection System; System, welches unter Verwendung verschiedener Methoden Angriffe auf ein IT-System entdecken kann

**IHP**

Incident Handling Plan; Dokument, welches die Vorgänge des Incident Handlings beschreibt und Handlungsweisen und Verantwortungen festlegt

**Incident Handling**

Aktivitäten, welche als Reaktion auf sicherheitsrelevante Ereignisse durchgeführt werden

**International Standards Organisation**

Die International Standards Organisation ist die weltweite Vereinigung nationaler Normungsinstitute.

**Internet Service Provider**

Unternehmen, welche anderen Unternehmen bzw. Privatpersonen den Zugang zum Internet ermöglicht und auch begleitende Dienstleistungen anbietet

**Impact**

Unter Impact versteht man die mittelbaren Auswirkungen eines Angriffs auf die Organisation; beispielsweise den Verlust von Kundenvertrauen oder finanzielle Schäden.

**IT-Control**

→ Control im Bereich der IT

**IT-Governance**

IT-Governance ist ein Organisationsmodell, welches der steigenden Wichtigkeit von IT-Systemen Rechnung trägt, indem es sie direkt in die Abläufe der Organisation integriert.

**ISACA**

Information Systems Audit and Control Association; 1967 durch eine Gruppe von Auditoren gegründet, um eine zentralisierte Quelle von Informationen und Richtlinien für ihren Geschäftsbereich zu schaffen. Heute hat die ISACA mehr als 35000 Mitglieder weltweit, setzt Standards im Bereich der IT-Sicherheits-Überprüfungen und stellt unter anderem Zertifikate in diesem Bereich aus. Im WWW: <http://www.isaca.org>

**ISP**

→ Internet Service Provider

**ISO**

→ International Standards Organisation

**Key Goal Indicators**

Die Key Goal Indicators definieren Indikatoren für das Management, ob ein IT-Prozess seine Business Requirements of Information erfüllt.

**Key Performance Indicators**

Die Key Performance Indicators definieren Indikatoren für das Management, wie die Performanz eines IT-Prozesses in Bezug auf die Erreichung der Business Requirements of Information ausfällt.

**KGIs**

→Key Goal Indicators

**KPIs**

→Key Performance Indicators

**Maßnahmenkatalog**

Unter einem Maßnahmenkatalog versteht man eine Sammlung von akzeptierten und erprobten Sicherheitsmaßnahmen und Vorgangsweisen, welche eine Organisation als Vergleich und Hilfe verwenden kann bzw. soll.

**Maturity Models**

Die Maturity Models sind ein Bewertungsmodell für die →IT-Control in der COBIT-Methodik.

**Monitoring**

Fortlaufende Überprüfung der IT-Systeme

**NASL**

Nessus Attack Scripting Language; Scriptsprache zur Entwicklung von Plug-Ins für den Schwachstellenscanner Nessus.

**OCTAVE<sup>SM</sup>**

Operationally Critical Threat, Asset, and Vulnerability Evaluation

**OCTAVE<sup>SM</sup> Attributes**

Die OCTAVE<sup>SM</sup> Attributes sind von den OCTAVE<sup>SM</sup> Principles abgeleitete, definierte Eigenschaften des IT-Sicherheits-Überprüfungsprozesses.

**OCTAVE<sup>SM</sup> Criteria**

Die OCTAVE<sup>SM</sup> Criteria sind die Vereinigung aus OCTAVE<sup>SM</sup> Principles, OCTAVE<sup>SM</sup> Attributes und OCTAVE<sup>SM</sup> Outputs. Sie definieren den Ablauf und die Eigenschaften einer IT-Sicherheits-Überprüfung, welche dem OCTAVE<sup>SM</sup>-Ansatz folgt.

**OCTAVE<sup>SM</sup> Principles**

Die OCTAVE<sup>SM</sup> Principles beschreiben die fundamentale Philosophie hinter dem OCTAVE<sup>SM</sup> Ansatz.

**OCTAVE<sup>SM</sup> Outputs**

Die OCTAVE<sup>SM</sup> Outputs sind die definierten Ergebnisse, welche aus den Phasen der OCTAVE<sup>SM</sup>-Methode hervorgehen müssen.

**Ö-IT-SIHB**

Österreichisches IT-Sicherheitshandbuch.

Ein an Behörden, Unternehmen und interessierte Privatpersonen gerichtetes Dokument in zwei Teilen, welches sich mit Security in umfassender Weise beschäftigt. Teil 1 beschreibt die Einrichtung eines umfassenden, kontinuierlichen IT-Sicherheitsmanagement-Prozesses. Teil 2 befasst sich mit grundlegenden organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen. Frei zum Download unter: [http://www.cio.gv.at/securenetworks/sihb/oe-it-sihb\\_v2\\_2\\_teil1.pdf](http://www.cio.gv.at/securenetworks/sihb/oe-it-sihb_v2_2_teil1.pdf) und [http://www.cio.gv.at/securenetworks/sihb/oe-it-sihb\\_v2\\_2\\_teil1.pdf](http://www.cio.gv.at/securenetworks/sihb/oe-it-sihb_v2_2_teil1.pdf)

**Outcome**

Unter Outcome versteht man die unmittelbaren Auswirkungen eines Angriffs auf die Sicherheitsanforderungen; beispielsweise den Verlust der Verfügbarkeit oder Vertraulichkeit von Daten.

**Schlüsselklasse**

Die Schlüsselklasse von Komponenten sind die Teile des System of Interest oder stehen mit ihm in Verbindung, also jene Teile, welche den Zugriff auf das System of Interest erlauben.

**Schwachstelle**

Unter einer Schwachstelle versteht man eine Sicherheitsschwäche eines Objektes oder IT-Systems, welche durch eine korrespondierende Bedrohung ausgenutzt werden kann.

**Security Awareness**

Sicherheitsbewusstsein bei den Benutzern eines IT-Systems

**Security Compliance Checking**

Prüfung der eingesetzten Sicherheitsmaßnahmen auf Übereinstimmung mit der IT-Sicherheitspolitik. Diese Prüfung wird bei der Umsetzung des IT-Sicherheitsplans, sowie danach in regelmäßigen Abständen bzw. nach Veränderungen der Maßnahmen oder der IT-Sicherheitspolitik durchgeführt.

**System of Interest**

Das System of Interest ist das System, welches einem Angreifer den Zugriff auf einen kritischen Unternehmenswert ermöglicht.

**Threat Profile**

→ Bedrohungsprofil

**Threat Tree**

→ Bedrohungsbaum

**WLAN**

Wireless LAN; Drahtlose Netzwerkverbindung nach IEEE 802.11

**WWW**

World Wide Web

## Anhang

**Anhang A: Literatur- und Quellenverzeichnis**

**Autor-Nachname, Autor-Vorname (Erscheinungsjahr):** *Titel. Untertitel.* ev. Auflage. Erscheinungsort: Verlag

**Symantec Corp. (2005):** *Symantec Internet Threat Report.* Symantec Corp.:  
<http://ses.symantec.com/pdf/ThreatReportVII.pdf>

**CERT®/CC (2004):** *CERT®/CC Statistics 1988-2004.* CERT®/CC:  
[http://www.cert.org/stats/cert\\_stats.html#incidents](http://www.cert.org/stats/cert_stats.html#incidents)

**Hahnbauer, Bernd (2003):** *Maßnahmen gegen Sicherheitslücken in Netzwerk-Infrastruktur-Komponenten.* Fachhochschulstudiengang Telekommunikation und Medien St. Pölten

**Chief Information Office, Stabsstelle IKT-Strategie des Bundes (2004):** *Österreichisches IT-Sicherheitshandbuch Teil 1.* Version 2.2.  
[http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB\\_V2\\_2\\_Teil1.pdf](http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB_V2_2_Teil1.pdf)

**Chief Information Office, Stabsstelle IKT-Strategie des Bundes (2004):** *Österreichisches IT-Sicherheitshandbuch Teil 2.* Version 2.2.  
[http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB\\_V2\\_2\\_Teil2\\_mit\\_Anhang\\_C.pdf](http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB_V2_2_Teil2_mit_Anhang_C.pdf)

**Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idF. BGBl. I Nr. 136/2001 (1999/2001):** Österreichische Datenschutzkommission: <http://www.dsk.gv.at>

**BSI - Bundesamt für Sicherheit in der Informationstechnik (2003):** *IT-Grundschriftshandbuch* Version von Juli 2003.  
<http://www.bsi.de/gshb/deutsch/download/GSHB2003.pdf>

**Alberts C. J. und Dorofee A. J. (2001):** *OCTAVE<sup>SM</sup> Criteria, Version 2.0*

**Alberts C. J. und Dorofee A. J. (2002):** *Managing Information Security Risks: The OCTAVE<sup>SM</sup> Approach.* Addison Wesley

**Alberts C. J., Dorofee A. J. und Allen J. H. (2001):** *OCTAVE<sup>SM</sup> Catalog of Practice, Version 2.0.*

**CERT®/CC (2003):** *OCTAVE® Information Security Risk Evaluation 2003.* CERT®/CC:  
<http://www.cert.org/octave/>

**IT Governance Institute (2000a):** *COBIT Executive Summary.* IT Governance Institute:  
<http://www.isaca.ch/files/CobitExecutiveSummary.pdf>

**IT Governance Institute (2000b):** *COBIT Management Guidelines.* IT Governance Institute:  
<http://www.isaca.ch/files/CobitManagementGuidelines.pdf>

**IT Governance Institute (2000c):** *COBIT Framework.* IT Governance Institute:  
<http://www.isaca.ch/files/CobitFramework.pdf>

**IT Governance Institute (2000d):** *COBIT Control Objectives.* IT Governance Institute:  
<http://www.isaca.ch/files/CobitKontrollzieleEnglisch.pdf>

**IT Governance Institute (2000e):** *COBIT Audit Guidelines.* IT Governance Institute

**ISACA Switzerland Chapter (1998):** *CoP, COBIT, Marion, Grundschriftshandbuch – Vier Methoden im Vergleich.* ISACA Switzerland Chapter:  
[http://www.isaca.ch/files/igcop\\_broschuere.pdf](http://www.isaca.ch/files/igcop_broschuere.pdf)

- Initi@tive D<sup>21</sup> (2001)** *IT-Sicherheitskriterien im Vergleich*. Initi@tive D<sup>21</sup>:  
[http://www.initiaved21.de/druck/news/publikationen2002/doc/22\\_1053502380.pdf](http://www.initiaved21.de/druck/news/publikationen2002/doc/22_1053502380.pdf)
- OCTAVE<sup>SM</sup> Information Centre & ATI Corp. (2005)**: *Risk Assessment Tool*:  
[http://oatool.aticorp.org/Tool\\_Info.html](http://oatool.aticorp.org/Tool_Info.html)
- ISO - International Organization for Standardization (2005)**: *ISO/IEC 17799:2000*:  
<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=&showrevision=y>
- ISO 17799 Information Security Group (2005)**: *ISO 17799 FAQ*: <http://www.iso-17799.com/faq.htm>
- BSI - Bundesamt für Sicherheit in der Informationstechnik (2003)**: *Studie Durchführungs-konzept für Penetrationstests*.  
<http://www.bsi.de/literat/studien/pentest/penetrationstest.pdf>
- Anonymous (2001)**: *Der neue Hacker's Guide. Sicherheit im Internet und im lokalen Netz*. Markt + Technik Verlag
- Insecure.org (2005)**: *Insecure.org - Nmap Free Security Scanner, Tools & Hacking resources*:  
<http://www.insecure.org>
- Anderson, Harry (28.10. 2003)**: *Introduction to Nessus*. SecurityFocus.  
<http://www.securityfocus.com/infocus/1741>
- Anderson, Harry (3.2. 2004)**: *Nessus, Part 3: Analysing Reports*. SecurityFocus.  
<http://www.securityfocus.com/infocus/1759>
- Internet Security Systems (2005)**: *Internet Security Systems - World Wide Homepage*  
<http://www.iss.net>
- Scheiderer, Jürgen (2004)**: *Sichere Basis – IT Grundschutz-Tool in neuer Version*. In: Seeger et al.: iX 9/2004. Heise
- Kismet (2005)**: *Kismet*. <http://www.kismetwireless.net>
- Wellenreiter (2005)**: *Wellenreiter – WaveLAN Hacking*.  
<http://www.wellenreiter.net/index.html>
- Remote Exploit (2005)**: *Rexploit*. <http://new.remote-exploit.org>

## **Anhang B: Abbildungsverzeichnis**

Abb. 1-1, VBS, 5.3.2004,

<http://www.vbs-ddps.ch/internet/groupgst/de/home/integrale0/objektschutz0.html>

Abb. 1-2 bis 1-5, **Chief Information Office, Stabsstelle IKT-Strategie des Bundes (2004): Österreichisches IT-Sicherheitshandbuch Teil 1**. Version 2.2.

[http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB\\_V2\\_2\\_Teil1.pdf](http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB_V2_2_Teil1.pdf)

Abb. 2-1 bis 2-7, **BSI - Bundesamt für Sicherheit in der Informationstechnik (2003): IT-Grundschriftbandbuch** Version von Juli 2003.

<http://www.bsi.de/gshb/deutsch/download/GSHB2003.pdf>

Abb. 2-8, **Alberts C. J. und Dorofee A. J. (2001): OCTAVE<sup>SM</sup> Criteria, Version 2.0**

Abb. 2-9, **Alberts C. J., Dorofee A. J. und Allen J. H. (2001): OCTAVE<sup>SM</sup> Catalog of Practice, Version 2.0**

Abb. 2-10 bis 2-13, **Alberts C. J. und Dorofee A. J. (2002): Managing Information Security Risks: The OCTAVE<sup>SM</sup> Approach**. Addison Wesley

Abb. 2-14 bis 2-16, 2-18 und 2-20, **IT Governance Institute (2000): CobIT Framework**

Abb. 2-16, 2-19 und F-1 bis F-2, **IT Governance Institute (2000): CobIT Management Guidelines**

Abb. 2-21 bis 2-24, **IT Governance Institute (2000): CobIT Audit Guidelines**

Abb. 3-1 bis 3-2 und G-1 bis G-2, **BSI – Bundesamt für Sicherheit in der Informationstechnik (2003): Studie Durchführungskonzept für Penetrationstest**

Abb. 4-1 und 4-2, **Autor**

Abb. E-1 bis E-4, **Alberts C. J. und Dorofee A. J. (2002): Managing Information Security Risks: The OCTAVE<sup>SM</sup> Approach**. Addison Wesley

## Anhang C: Schadensgrenzen für Schutzbedarfskategorien nach IT-GSHB

Schutzbedarfskategorie „niedrig bis mittel“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen - Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. - Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.
5. Negative Außenwirkungen	- Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden bleibt für die Institution tolerabel.

Quelle: GSHB, S. 44

Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen - Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von einzelnen Betroffenen als

	nicht tolerabel eingeschätzt. - Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Außenwirkungen	- Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	- Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Quelle: GSHB, S. 44f

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	- Fundamentaler Verstoß gegen Vorschriften und Gesetze - Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	- Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. - Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
3. Beeinträchtigung der persönlichen Unversehrtheit	- Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. - Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	- Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. - Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Außenwirkungen	- Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	- Der finanzielle Schaden ist für die Institution existenzbedrohend.

Quelle: GSHB, S. 45

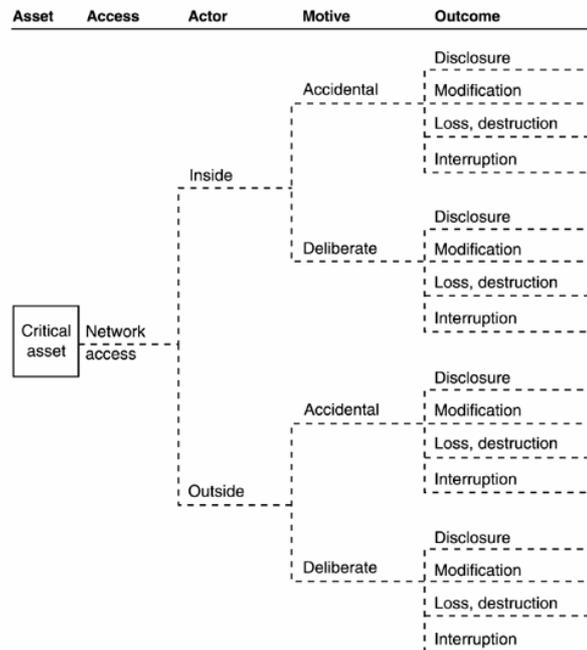
**Anhang D: Zurdnung der OCTAVE<sup>[SM]</sup> Attributes zu den OCTAVE<sup>[SM]</sup> Principles**

Principles	Attributes
Self-direction	Analysis team Augmenting analysis team skills
Adaptable measures	Catalog of practices Generic threat profile Catalog of vulnerabilities
Defined process	Defined evaluation activities Documented evaluation results Evaluation scope
Foundation for a continuous process	Next steps Catalog of practices Senior management participation
Forward-looking view	Focus on risk
Focus on the critical few	Evaluation scope Focused activities
Integrated management	Organizational and technological issues Business and information technology participation Senior management participation
Open communication	Collaborative approach
Global perspective	Organizational and technological issues Business and information technology participation

Principles	Attributes
Teamwork	Analysis team  Augment analysis team skills  Business and information technology participation  Collaborative approach

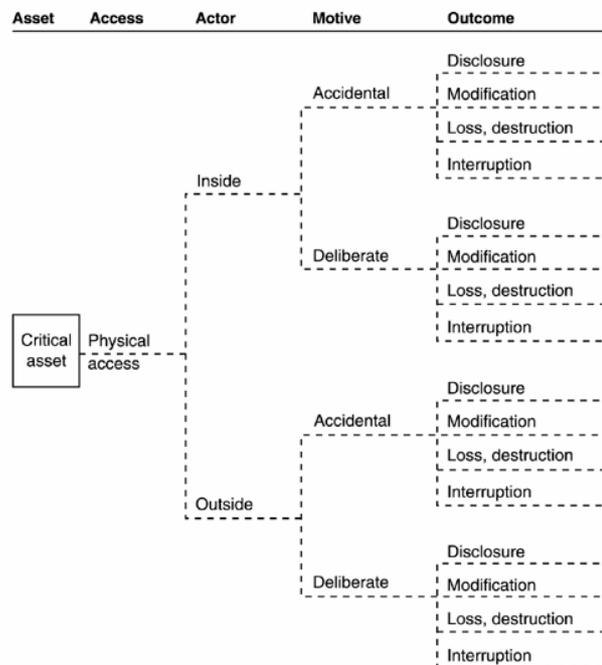
Quelle: Alberts & Dorofee 2002

## Anhang E: OCTAVE[SM] Bedrohungsbaume



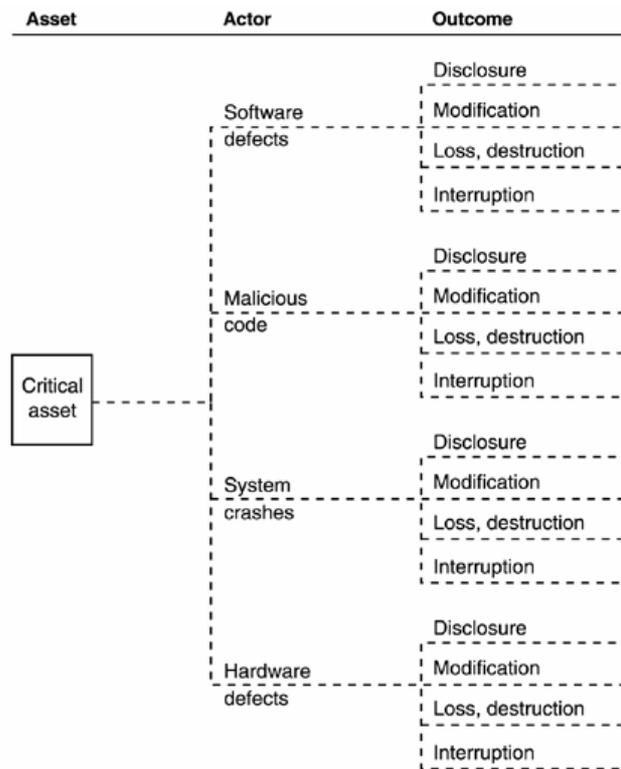
**Abbildung E-1: OCTAVE<sup>SM</sup> Bedrohungsbaum für menschliche Akteure über Netzwerkzugriff**

Quelle: Alberts & Dorofee 2002, Kap. B.2



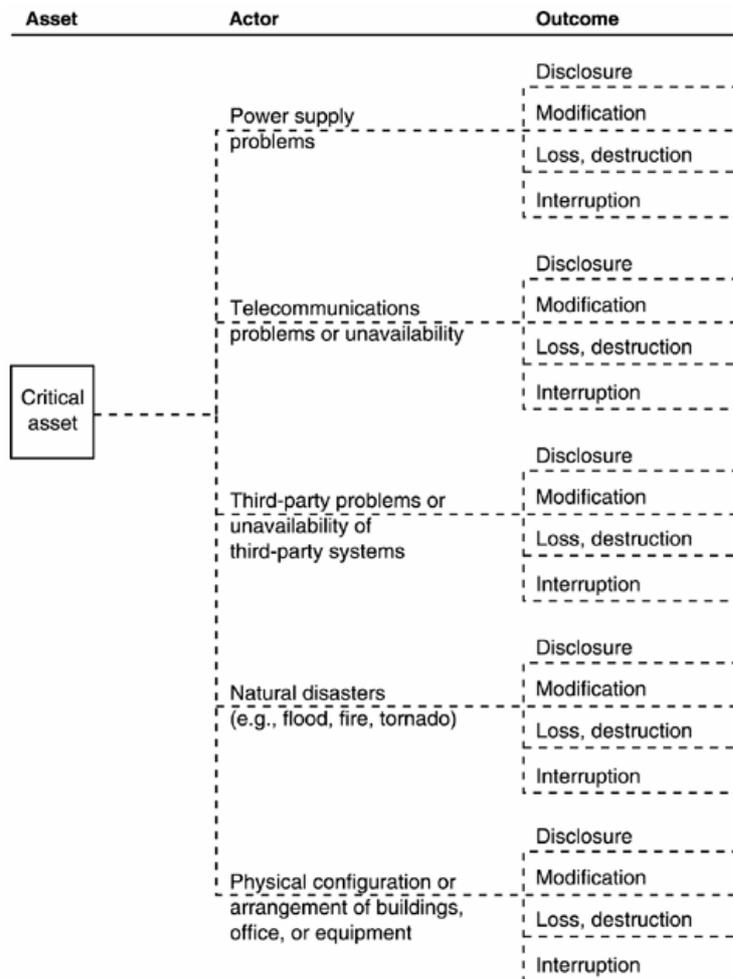
**Abbildung E-2: OCTAVE<sup>SM</sup> Bedrohungsbaum für menschliche Akteure über physikalischen Zugriff**

Quelle: Alberts & Dorofee 2002, Kap. B.2



**Abbildung E-3: OCTAVE<sup>SM</sup> Bedrohungsbaum für Systemprobleme**

Quelle: Alberts & Dorofee 2002, Kap. B.2



**Abbildung E-4: OCTAVE<sup>SM</sup> Bedrohungsbaum für andere Probleme**

Quelle: Alberts & Dorofee 2002, Kap. B.2

## Anhang F: Beispiel für eine COBIT Management Guideline

### M4 Monitoring Provide for Independent Audit COBIT

Control over the IT process **Provide for Independent Audit** with the business goal of *increasing confidence levels and benefit from best practice advice*

ensures delivery of information to the business that addresses the required **Information Criteria** and is measured by **Key Goal Indicators**

is enabled by *independent audits carried out at regular intervals*

considers **Critical Success Factors** that leverage specific **IT Resources** and is measured by **Key Performance Indicators**

#### Information Criteria

P	effectiveness
P	efficiency
S	confidentiality
S	integrity
S	availability
P	compliance
S	reliability

(P) primary (S) secondary

#### IT Resources

✓	people
✓	applications
✓	technology
✓	facilities
✓	data

(✓) applicable to

#### Key Goal Indicators

- Increased level of confidence derived from independent audit activities
- Increased adoption of best practices as a result of independent audit advice and recommendations
- Increased value for the money
- Increased level of communication with the audit committee and senior management

#### Critical Success Factors

- An audit committee that defines and supports an audit mandate that provides for the independence, responsibility, authority and accountability of the audit function
- Risk-based planning is used to identify business and IT activities for initial and cyclical reviews
- The planning and conducting of audits are proactive
- The audit methodology is properly supported by tools and techniques
- Clearly-agreed on practices between management and audit are established for tracking and closing audit recommendations and for reporting on global status
- Auditors perform impact assessments of recommendations, including cost, benefit and risk
- Audits are performed in accordance with generally accepted auditing standards

#### Key Performance Indicators

- Increased level of satisfaction with the audit function working relationship
- Number of corrective and sustainable actions taken as a result of new audit findings
- Increased number of auditors with professional and technical certifications
- Improved cycle time of the audit process, from planning through reporting

**Abbildung F-1: CSFs, KGIs und KPIs für die COBIT Management Guideline für den IT-Prozess M4 1/2**

Quelle: IT Governance Institute, 2000b, S. 96

# MANAGEMENT GUIDELINES

## M4

### M4 Maturity Model

Control over the IT process **Provide for Independent Audit** with the business goal of *increasing confidence levels and benefit from best practice advice*

- 0 **Non-existent** Management is unaware of the importance of an independent audit function and independent audits do not take place.
- 1 **Initial/Ad Hoc** An informal IT audit function exists which carries out independent reviews from time to time. There is no overall plan for providing independent audits and no co-ordination between reviews. Independent audit planning, managing and reporting are based on individual expertise. The quality of planning and delivery of audit services is generally poor, with variable results and very limited management involvement.
- 2 **Repeatable but Intuitive** Provision of an independent audit function is recognised by management as being potentially useful, but there is no written policy defining its purpose, authority and responsibilities. Senior management has not established an infrastructure and process to ensure that independent audits are performed on a regular basis. Independent audit planning, managing and reporting follows a similar pattern, based on previously gained experience and the expertise of the team members. There is little co-ordination between audits and limited follow-up of previous audit findings. IT management interest and involvement in the audit process is inconsistent and dependent on the perceived quality of the specific audit team.
- 3 **Defined Process** A charter for the IT audit function is established by senior management and followed in providing for the independence and authority of the audit function. Audit management has identified and understands the IT environment and initiatives. A process is established for planning and managing audits. Audit staff is expected to comply with auditing standards, but results may be variable. Resolution of audit comments does occur, but often there is poor follow-up and closure. Basic elements of quality assurance are established to assure that practices comply with applicable auditing standards and to improve the

effectiveness of audit function activities. The IT, financial and process audit functions are not generally integrated. IT management is aware of the need for independent audits, but is not always satisfied with the quality provided and does not have confidence that the function has adequate knowledge to make valid recommendations.

- 4 **Managed and Measurable** Strategic and operational risk-based audit plans are established, based on an assessment of current and future needs. Individual audit plans are developed, based on a cyclical operational plan and resource availability. The audit process can be tailored to specific assignments. A process knowledge base is established and is developed to ensure that quality assessments can be made and useful recommendations are generated. Audits are co-ordinated and integrated with any associated financial and process audits. Results are reported to management and follow-up occurs to ensure that management has taken corrective actions on critical issues identified by the audits. A structured quality assurance function facilitates quantitative management and control of the audit process. The IT audit function participates in the development of corrective actions and in projects to ensure that controls are appropriately built into processes. IT management is usually positively involved in all audits and makes use of audit results to improve performance.
- 5 **Optimised** The audit function is capable of rapidly responding to management concerns related to business process and IT control risk issues on a continuous, organisation-wide basis. Audit planning is closely integrated with business and IT strategies. Audit processes are monitored and analysed for improvement in adapting to changing environmental conditions. This includes quantitatively monitoring activities in the auditing community and taking into account state-of-the-art industry best practices and other external trends in adjusting auditing processes. Audit is involved in the development of business plans and in all projects that support business plans, to ensure that the appropriate controls are included into all processes. Audit is consulted on all projects for control and business advice.

### Abbildung F-2: Maturity Model für die COBIT Management Guideline für den IT-Prozess M4 2/2

Quelle: IT Governance Institute, 2000b, S. 97

Anhand dieses Beispiels ist ersichtlich, wie die zuerst die IT-Control über den betreffenden IT-Prozess definiert wird, und anschließend die Management Guidelines des IT-Prozesses beschrieben werden. Darüber hinaus wird wie in den COBIT Control Objectives angeführt,

auf welche Business Requirements of Information (Information Criteria) der Prozess primär bzw. sekundär Einfluss nimmt, sowie auf welche IT-Ressourcen er anwendbar ist.

**Anhang G: Module für die Durchführung eines Penetrationstests**

<i>Nr.</i>	<i>Modulbezeichnung</i>
I 1	Auswertung öffentlich zugänglicher Daten
I 2	Verdeckte Abfragen von Netzwerkbasisinformationen
I 3	Offensichtliche Abfragen von Netzwerkbasisinformationen
I 4	Verdeckte Durchführung von Portscans
I 5	Offensichtliche Durchführung von Portscans
I 6	Identifikation von Anwendungen
I 7	Identifikation von Systemen
I 8	Verdeckte Identifikation der Router
I 9	Offensichtliche Identifikation der Router
I 10	Verdeckte Identifikation der Firewalls
I 11	Offensichtliche Identifikation der Firewalls
I 12	Recherche nach Schwachstellen
I 13	Identifikation von Anwendungsschnittstellen
I 14	Sammlung von Informationen für Social-Engineering
I 15	Sammlung von Informationen für computerbasiertes Social-Engineering
I 16	Sammlung von Informationen für persönliches Social-Engineering
I 17	Überprüfung der drahtlosen Kommunikation (nur scannend)
I 18	Test der Telefonanlage (Identifikation)
I 19	Test des Voicemailsystems (Identifikation)
I 20	Test des Faxsystems (Identifikation)
I 22	Identifikation von Zutrittskontrollen
I 21	Analyse der physischen Umgebung
I 22	Identifikation von Zutrittskontrollen

**Abbildung G-1: I-Module / Module zur Informationsbeschaffung**

Quelle: BSI 2003, S. 49

<i>Nr.</i>	<i>Modulbezeichnung</i>
E 1	Verdeckte Verifikation tatsächlicher Schwachstellen
E 2	Offensichtliche Verifikation tatsächlicher Schwachstellen
E 3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen
E 4	Verdeckter Test der Router
E 5	Offensichtlicher Test der Router
E 6	Test von Vertrauensbeziehungen zwischen Systemen
E 7	Verdeckter Test der Firewall von außen
E 8	Offensichtlicher Test der Firewall von außen
E 9	Beidseitiger Test der Firewall
E 10	Test des IDS-Systems
E 11	Abhören von Passwörtern
E 12	Test von Passwörtern
E 13	Test von „Denial-of-Service“ Anfälligkeit
E 14	Computerbasiertes Social-Engineering
E 15	Direktes, persönliches Social-Engineering mit physischem Zutritt
E 16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt
E 17	Überprüfung der drahtlosen Kommunikation
E 18	Test der administrativen Zugänge zur Telefonanlage
E 19	Test des Voicemailsystems
E 20	Test der administrativen Zugänge zum Faxsystems
E 21	Test von Modems
E 22	Aktiver Test der Zutrittskontrollen
E 23	Überprüfung der Eskalationsprozeduren

**Abbildung G-2: E-Module / Module für aktive Eindringversuche**

Quelle: BSI 2003, S. 50

**Anhang H: Fragebogen zur Klärung des Dienstleistungsangebots für IT-Sicherheits-Überprüfungen**

1.	Bietet Ihr Unternehmen Sicherheitsüberprüfungen von IT Infrastrukturen an?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2
2.	Auf welche Kunden ist Ihr Angebot zugeschnitten?		
A	Klein- und mittelständische Unternehmen	<input type="checkbox"/>	1
B	Große Unternehmen/Konzerne	<input type="checkbox"/>	2
C	Unternehmen/Organisationen mit besonderen Sicherheitsvorgaben (z.B. Banken, staatliche Einrichtungen, etc.)	<input type="checkbox"/>	3
3.	Bilden Sicherheitsüberprüfungen ein Kerngeschäft Ihres Unternehmens?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2
4.	Wie lautet die Bezeichnung für Ihr Dienstleistungsangebot?		
5.	Auf welche Arten von Infrastrukturen ist Ihr Angebot zugeschnitten? (WAN/LAN/WLAN/Telefonanlagen/...) <u>Mehrfachnennungen möglich</u>		
6.	Beschränkt sich Ihr Angebot auf bestimmte Applikationen?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2
	Wenn ja, welche? (Datenbanken/Webserver/spezielle) <u>Mehrfachnennungen möglich</u>		
7.	Beschränkt sich Ihr Angebot auf bestimmte Systeme?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2
	Wenn ja, welche? (Windows/Unix/Linux/Internetsysteme/spezielle) <u>Mehrfachnennungen möglich</u>		

8.	Welche Methoden kommen bei Ihrem Angebot zur Anwendung?		
A	Externe Sondierung (Portscanning, Security Scanning, etc.)	<input type="checkbox"/>	1
B	Interne Sondierung	<input type="checkbox"/>	2
C	Gezielter externer Angriffsversuch	<input type="checkbox"/>	3
D	Gezielter interner Angriffsversuch	<input type="checkbox"/>	4
E	Sichten der Systemkonfigurationen	<input type="checkbox"/>	5
F	Prüfung der technischen Sicherheit (Systeme)	<input type="checkbox"/>	6
G	Prüfung der organisatorischen Sicherheit (Policies)	<input type="checkbox"/>	7
9.	Welche der folgenden Aspekte der IT Security werden in Ihrem Angebot überprüft?		
A	Perimetersicherheit (externe Sicherheit)	<input type="checkbox"/>	1
B	Interne Sicherheit	<input type="checkbox"/>	2
C	Gebäudesicherheit (Zugangskontrolle, etc.)	<input type="checkbox"/>	3
D	Sicherheit gegenüber Viren und Trojanern	<input type="checkbox"/>	4
E	Sicherheit der aktiven Komponenten (Router, Switches, etc.)	<input type="checkbox"/>	5
F	Application Security (Sicherheit der verwendeten Applikationen)	<input type="checkbox"/>	6
G	Desktop Security (Sicherheit der Desktopsysteme gegen unbefugten Zugriff)	<input type="checkbox"/>	7
H	Personalsicherheit (Einhaltung der Policies durch die Angestellten)	<input type="checkbox"/>	8
I	Verantwortliche Personen (Einhaltung und Durchsetzung der Policies durch die zuständigen Personen)	<input type="checkbox"/>	9
10.	Welche Werkzeuge kommen bei Ihrem Angebot zur Anwendung?		
A	Kommerzielle Tools	<input type="checkbox"/>	1
B	Freie Tools	<input type="checkbox"/>	2
	Bitte nennen Sie die hauptsächlich verwendeten Tools:		
11.	Welches ist der Mindestaufwand an Kosten und Dauer einer Überprüfung, eingeschränkt auf wie viele Systeme bzw. IP Adressen?		
12.	Enthält Ihr Angebot Verbesserungsvorschläge für die IT Security?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2

C	Ja, gegen Aufpreis	<input type="checkbox"/>	3
13.	Enthält Ihr Angebot Unterstützung bei der Verbesserung des Sicherheitsstandards?		
A	Nein	<input type="checkbox"/>	1
B	Ja	<input type="checkbox"/>	2
C	Ja, gegen Aufpreis	<input type="checkbox"/>	3