

# BSI FOREIGN DOCUMENTS

# Ü B E R S E T Z U N G

BS 7799-1  
1999

Management von Informationssicherheit –

Teil 1: Leitfaden zum Management von Informationssicherheit

*original language Version  
Information security management -  
Part 1: Code of practice for information  
security management*

---

*Issued by  
British Standards Institution  
389 Chiswick High Road  
London  
W44AL*

---

BSI Foreign Documents has taken all reasonable measures to ensure the accuracy of this translation but regrets that no responsibility can be accepted for any error, omission or inaccuracy.  
In cases of doubt or dispute, the original language text only is valid.

© BSI Foreign Documents  
389 Chiswick High Road, London W4 4AL  
Tel: +44 208 996 7525  
Facsimile: +44 208 996 7121

The British Standards Institution is incorporated by Royal Charter

## **Ausschüsse, die für diese Britische Norm verantwortlich sind:**

Die Vorbereitung dieser Britischen Norm wurde dem BSI/DISC Committee BDD/2, Management von Informationssicherheit, übertragen, in dem die folgenden Organisationen vertreten waren:

Association of British Insurers  
British Computer Society  
British Telecommunications plc  
The Business Continuity Institute  
Department of Trade and Industry (Information Security Policy Unit)  
Det Norske Veritas Quality Assurance  
HMG Protective Security Authority  
HSBC  
Indicii Salus  
Institute of Chartered Accountants in England and Wales  
Institute of Internal Auditors  
KPMG plc  
L3 Network Security  
Lloyds TSB  
Logica UK  
Marks & Spencer plc  
Nationwide Building Society  
PCSL  
Racal Network Services  
RKP Associates  
Shell International Petroleum Co Ltd  
Unilever plc  
Whitbread plc  
XiSEC Consultants Ltd/AEXIS Consultants

Diese Britische Norm, die unter der Leitung des DISC Board erarbeitet wurde,  
erschien mit Genehmigung des Standards Board und gilt ab 15. Mai 1999.

©BSI 05-1999

Veröffentlicht zum ersten Mal als BS 7799 in Februar 1995  
Veröffentlicht als BS 7799-1 in Februar 1998

Die folgenden BSI-Verweise beziehen sich auf die Arbeit bezüglich dieser Norm:  
Ausschußverweis BDD/2  
Kommentarentwurf 98/682025 DC

Vorgenommene Änderungen seit Erscheinen dieser Norm  
Änd. Nr.:  
Datum:  
Geänderter Text:

# Inhaltsverzeichnis

	Seite
Verantwortliche Ausschüsse .....	Titelrückseite
Vorwort .....	iii
Einleitung .....	1
<b>1 ANWENDUNGSBEREICH.....</b>	<b>5</b>
<b>2 BEGRIFFE UND DEFINITIONEN.....</b>	<b>5</b>
2.1 INFORMATIONSSICHERHEIT .....	5
2.2 RISIKOANALYSE .....	5
2.3 RISIKOMANAGEMENT.....	5
<b>3 SICHERHEITSPOLITIK .....</b>	<b>5</b>
3.1 INFORMATIONSSICHERHEITSPOLITIK.....	5
<b>4 ORGANISATION DER SICHERHEIT .....</b>	<b>7</b>
4.1 INFRASTRUKTUR DER INFORMATIONSSICHERHEIT .....	7
4.2 SICHERHEIT BEI DEM ZUGANG DURCH FREMDUNTERNEHMEN .....	10
4.3 OUTSOURCING.....	13
<b>5 EINSTUFUNG UND KONTROLLE DER WERTE.....</b>	<b>14</b>
5.1 ZURECHENBARKEIT FÜR WERTE.....	14
5.2 EINSTUFUNG VON INFORMATIONEN .....	15
<b>6 PERSONELLE SICHERHEIT .....</b>	<b>16</b>
6.1 SICHERHEIT BEI DER STELLENBESCHREIBUNG UND BEI DER BEREITSTELLUNG VON RESSOURCEN .....	16
6.2 BENUTZERSCHULUNG .....	18
6.3 VERHALTEN BEI SICHERHEITSVorfällen UND Störungen .....	19
<b>7 PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT .....</b>	<b>20</b>
7.1 SICHERHEITZONEN .....	20
7.2 SICHERHEIT DER GERÄTE.....	24
7.3 ALLGEMEINE MAßNAHMEN .....	27
<b>8 MANAGEMENT DER KOMMUNIKATION UND DES BETRIEBS.....</b>	<b>28</b>
8.1 BETRIEBSVERFAHREN UND -VERANTWORTLICHKEITEN .....	28
8.2 SYSTEMPLANUNG UND -ABNÄHME.....	33
8.3 SCHUTZ VOR BÖSARTIGER SOFTWARE .....	34
8.4 HAUSHALTSORGANISATION.....	35
8.5 NETZWERKMANAGEMENT .....	37
8.6 UMGANG MIT UND SICHERHEIT VON DATENTRÄGERN .....	37
8.7 AUSTAUSCH VON INFORMATIONEN UND SOFTWARE.....	40
<b>9 ZUGANGSKONTROLLE .....</b>	<b>45</b>
9.1 GESCHÄFTSANFORDERUNGEN AN DIE ZUGANGSKONTROLLE .....	45
9.2 VERWALTUNG DER ZUGRIFFSRECHTE DER BENUTZER .....	46
9.3 VERANTWORTUNG DER BENUTZER .....	49
9.4 NETZZUGRIFFSKONTROLLE .....	50
9.5 KONTROLLE DES BETRIEBSSYSTEMZUGRIFFS .....	54
9.6 ZUGRIFFSKONTROLLE FÜR ANWENDUNGEN .....	58
9.7 ÜBERWACHUNG DES SYSTEMZUGRIFFS UND DER SYSTEMBENUTZUNG .....	59
9.8 MOBILE COMPUTING UND TELEARBEIT.....	62
<b>10 SYSTEMENTWICKLUNG UND -WARTUNG .....</b>	<b>64</b>

**BS 7799-1:1999**

10.1	SICHERHEITSANFORDERUNGEN AN SYSTEME .....	64
10.2	SICHERHEIT IN ANWENDUNGSSYSTEMEN .....	65
10.3	KRYPTOGRAPHISCHE MAßNAHMEN .....	67
10.4	SICHERHEIT VON SYSTEMDATEIEN .....	71
10.5	SICHERHEIT BEI ENTWICKLUNGS- UND SUPPORTPROZESSEN.....	73
11	MANAGEMENT DES KONTINUIERLICHEN GESCHÄFTSBETRIEBS .....	<b>76</b>
11.1	ASPEKTE ZUR AUFRECHTERHALTUNG DES GESCHÄFTSBETRIEBS .....	76
12	EINHALTUNG DER VERPFLICHTUNGEN .....	<b>80</b>
12.1	EINHALTUNG GESETZLICHER VERPFLICHTUNGEN.....	80
12.2	ÜBERPRÜFUNGEN DER SICHERHEITSPOLITIK UND DER EINHALTUNG TECHNISCHER NORMEN .....	85
12.3	ÜBERLEGUNGEN ZUM SYSTEMAUDIT .....	86
<b>Anhang A (informativ) Änderungen bei der internen Numerierung</b>		87
<b>Stichwortverzeichnis</b>		89

## **Vorwort**

Dieser Teil der Norm BS 7799 wurde unter Aufsicht des BSI/DISC-Ausschusses BDD/2, Informationssicherheitsmanagement, aufgestellt. Er ersetzt die Norm BS 7799:1995, die zurückgezogen wurde.

Die Norm BS 7799 wird in zwei Teilen herausgegeben:

- Teil 1: Leitfaden zum Management von Informationssicherheit
- Teil 2: Spezifikation für Managementsysteme für Informationssicherheit

Die Norm BS 7799-1 wurde 1995 das erste Mal herausgegeben, um eine umfassende Sammlung von Maßnahmen bereitzustellen, in der die besten Praktiken in der Informationssicherheit enthalten sind. Sie soll gemeinsamer Bezugspunkt zur Identifizierung der verschiedenen Maßnahmen sein, die für die meisten Situationen erforderlich sind, in denen Informationssysteme in Industrie und Handel verwendet werden, und deshalb in großen, mittleren und kleineren Organisationen zum Einsatz kommen. Der Begriff Organisation wird in dieser Norm durchgängig verwendet und bezeichnet gleichzeitig Organisationen mit und ohne Erwerbscharakter sowie Organisationen der öffentlichen Hand.

In der überarbeiteten Fassung von 1999 werden die neuesten Entwicklungen in der Anwendung von Informationsverarbeitung berücksichtigt, insbesondere Netzwerke und Kommunikationstechnologie. Außerdem wird die Beteiligung von Unternehmen an der Informationssicherheit und ihre Verantwortung dafür stärker betont.

Nicht alle in diesem Dokument beschriebenen Maßnahmen sind für jede Situation relevant. Beschränkungen, die sich aus dem lokalen System, aus umgebungsspezifischen oder technologischen Gesichtspunkten ergeben, können nicht berücksichtigt werden. Ihre Formulierung ist u.U. nicht für jeden potentiellen Anwender in einer Organisation geeignet. Infolgedessen bedarf dieses Dokument eventuell einer Ergänzung durch weitere Richtlinien. Es kann beispielsweise als Grundlage für die Entwicklung einer Unternehmenspolitik oder für ein Geschäftsabkommen zwischen verschiedenen Unternehmen herangezogen werden.

Da es sich um einen Leitfaden handelt, werden in dieser Britischen Norm Richtlinien und Empfehlungen ausgesprochen. Sie sollte deswegen nicht so zitiert werden, als würde es sich um eine Spezifikation handeln. Außerdem ist besonders darauf zu achten, dass durch den Anspruch auf ihre Einhaltung keine Missverständnisse hervorgerufen werden.

Beim Entwurf dieser Norm wurde davon ausgegangen, dass die Ausführung der Bestimmungen entsprechend qualifizierten und erfahrenen Personen übertragen wird.

Anhang A hat informativen Charakter und enthält eine Tabelle, in der die Beziehung zwischen den Teilen der Ausgabe von 1995 und den Punkten der Ausgabe von 1999 aufgezeigt wird.

Eine Britische Norm gibt nicht vor, alle notwendigen Bestimmungen eines Vertrages zu enthalten. Benutzer von Britischen Normen sind selbst für deren richtige Anwendung verantwortlich.

**Die Einhaltung einer Britischen Norm allein entbindet den Anwender nicht von seinen gesetzlichen Verpflichtungen.**

## Einleitung

### Informationssicherheit

Informationen sind Werte, die genauso wie die übrigen Geschäftswerte wertvoll für eine Organisation sind und infolgedessen in geeigneter Weise geschützt werden müssen. Informationssicherheit schützt Informationen vor einer Vielzahl von Bedrohungen. Sie soll die Aufrechterhaltung des Geschäftsbetriebs gewährleisten, geschäftsschädigende Einflüsse niedrig halten sowie die Investitionsrentabilität und die Geschäftsgelegenheiten maximieren.

Informationen können in vielen Formen vorliegen. Sie können ausgedruckt, auf Papier geschrieben, elektronisch gespeichert, auf dem Postweg oder elektronisch übertragen, in Filmen gezeigt oder in Gesprächen mündlich weitergegeben werden. Informationen sollten unabhängig von der dargebotenen Form, der gemeinsamen Nutzung oder Speicherung immer angemessen geschützt werden.

Informationssicherheit wird hier verstanden als Sicherung der:

- a) Vertraulichkeit: Gewährleistung des Zugangs<sup>1</sup> zu Informationen nur für die Zugangsberechtigten;
- b) Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden;
- c) Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer;

Informationssicherheit wird durch die Implementierung von geeigneten Maßnahmen erzielt, die Politiken, Praktiken, Verfahren, Organisationsstrukturen und Softwarefunktionen sein können. Diese Maßnahmen sind zur Erfüllung der spezifischen Sicherheitsziele der Organisation festzulegen.

### Notwendigkeit der Informationssicherheit

Informationen und die sie unterstützenden Prozesse, Systeme und Netzwerke sind wichtige Geschäftswerte. Ihre Vertraulichkeit, Integrität und Verfügbarkeit können wesentlich zur Erhaltung von Wettbewerbsvorsprung, Liquidität, Rentabilität, Einhaltung gesetzlicher Vorschriften und Geschäftsansetzen beitragen.

Organisationen und ihre Informationssysteme und -netzwerke sehen sich Sicherheitsbedrohungen unterschiedlichster Herkunft, einschließlich Computerbetrugs, Spionage, Sabotage, Vandalismus, Feuers oder Überschwemmung, gegenüber. Gefahrenquellen wie Computerviren, Hacker und "Denial of Service"-Attacken werden immer verbreiteter, anspruchsvoller und raffinierter.

Die Abhängigkeit von Informationssystemen und -diensten bedeutet, dass Organisationen gegenüber Sicherheitsbedrohungen anfälliger sind. Die Verbindung von öffentlichen und privaten Netzwerken und die gemeinsame Nutzung von Informationsressourcen erhöhen die Schwierigkeit, eine effektive Zugangskontrolle zu gewährleisten. Der Trend hin zur verteilten Verarbeitung hat die Effektivität einer zentralen, fachlichen Kontrolle geschwächt.

---

<sup>1</sup> Zugang beschreibt hier und im folgenden sowohl den physischen wie auch den logischen Zugang.

Viele Informationssysteme sind nicht auf Sicherheit hin ausgelegt. Die technisch erzielbare Sicherheit ist begrenzt und sollte durch entsprechendes Management und entsprechende Verfahren unterstützt werden. Die Identifizierung der benötigten Maßnahmen erfordert sorgfältige Planung und Detailgenauigkeit. Beim Informationssicherheitsmanagement ist die Mitwirkung aller Beschäftigten in der Organisation eine Mindestvoraussetzung. Außerdem kann auch die Mitwirkung von Zulieferern, Kunden oder Anteilseignern erforderlich sein. Das Gleiche gilt auch für eine Fachberatung durch externe Organisationen.

Maßnahmen für die Informationssicherheit sind wesentlich kostengünstiger und effektiver, wenn sie in den Stadien der Anforderungsspezifikation und der Entwicklung integriert werden.

## Definition der Sicherheitsanforderungen

Es ist äußerst wichtig, dass eine Organisation ihre Sicherheitsanforderungen identifiziert. Drei Quellen sind hierbei von wesentlicher Bedeutung.

Die erste Quelle entspringt aus der Analyse der Risiken für die Organisation. Eine Risikoanalyse ermöglicht die Identifikation von Bedrohungen für die Werte, die Bewertung der Schwachstellen und der Wahrscheinlichkeit des Auftretens eines Risikos sowie die Analyse der möglichen Auswirkungen.

Die zweite Quelle sind die Anforderungen, die sich aus Gesetzen, Politik, Richtlinien und Verträgen ergeben, die von einer Organisation, ihren Handelspartnern, Auftragnehmern und Diensteanbietern (Service Provider) erfüllt werden müssen.

Die dritte Quelle sind die spezifischen Prinzipien, Ziele und Anforderungen der Informationsverarbeitung, die eine Organisation zur Unterstützung ihrer Abläufe entwickelt hat.

## Analyse der Sicherheitsrisiken

Sicherheitsanforderungen werden durch eine methodische Analyse der Sicherheitsrisiken identifiziert. Der Aufwand für Maßnahmen muss gegenüber dem wirtschaftlichen Schaden, der sich aus Sicherheitsversagen ergibt, abgewogen werden. In den Fällen, in denen dies durchführbar, realistisch und nützlich ist, können sich die Verfahren zur Risikoanalyse auf die gesamte Organisation oder nur auf Teile davon, oder auch auf einzelne Informationssysteme, spezifische Systemkomponenten oder -dienste erstrecken.

Risikoanalyse besteht in der systematischen Betrachtung folgender Punkte:

- a) Schaden für das Geschäft, der unter Berücksichtigung der potentiellen Folgen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen und anderer Werte möglicherweise durch einen Sicherheitsausfall entstehen kann;
- b) realistische Wahrscheinlichkeit, dass ein derartiger Ausfall angesichts der existierenden Bedrohungen und Schwachstellen und der derzeit implementierten Maßnahmen auftritt.

Die Ergebnisse dieser Analyse unterstützen die Beratung und Bestimmung der angemessenen Management-Aktion sowie der Prioritäten bei der Verwaltung von Informationssicherheitsrisiken und bei der Implementierung der zum Schutz gegen diese Risiken ausgewählten Maßnahmen. Der Prozess der Analyse von Risiken und der Auswahl von Maßnahmen muss u.U. mehrfach durchgeführt werden, um die verschiedenen Teile der Organisation oder des jeweiligen Informationssystems zu erfassen.

Es ist wichtig, periodische Überprüfungen der Sicherheitsrisiken und der implementierten Maßnahmen durchzuführen, um:

- a) Änderungen der Geschäftsanforderungen und -Prioritäten zu berücksichtigen;
- b) neue Bedrohungen und Schwachstellen zu ermitteln;
- c) Wirksamkeit und Angemessenheit der Maßnahmen zu bestätigen.

Die Überprüfungen sollten in Abhängigkeit der Ergebnisse früherer Analysen und dem sich ändernden Risikoniveau, das das Management zu tragen bereit ist, auf unterschiedlichen Stufen durchgeführt werden. Als ein Mittel zur Schwerpunktbildung von Ressourcen in Bereichen mit hohem Risiko wird eine Risikoanalyse häufig zuerst auf hoher Stufe ausgeführt, um dann auf einer detaillierteren Stufe spezifische Risiken anzugehen.

## Auswahl von Maßnahmen

Nach der Identifizierung von Sicherheitsanforderungen sollten auch Maßnahmen ausgewählt und implementiert werden, um sicherzustellen, dass Risiken auf ein annehmbares Niveau reduziert werden. Maßnahmen können aus diesem Dokument oder aus anderen Maßnahmenübersichten ausgewählt werden. Um spezifische Erfordernisse zu erfüllen, können nach Bedarf auch neue Maßnahmen festgelegt werden. Es gibt verschiedene Arten des Risikomanagements. Dieses Dokument stellt Beispiele für allgemein übliche Ansätze vor. Allerdings muss man sich darüber im klaren sein, dass einige Maßnahmen nicht für jedes Informationssystem oder für jede Umgebung geeignet und daher nicht von allen Organisationen umsetzbar sind. Beispielsweise wird in 8.1.4 beschrieben, wie Pflichten aufgeteilt werden können, um Betrug und Irrtum zu verhindern. Kleinere Organisationen sind u.U. nicht in der Lage, alle Pflichten aufzuteilen, so dass andere Wege zum Erreichen des gleichen Sicherheitsziels erforderlich sein könnten.

Die Maßnahmen sollten auf der Grundlage der Implementierungskosten im Verhältnis zu den dadurch reduzierten Risiken und den bei einem Sicherheitsverstoß auftretenden potentiellen Verlusten ausgewählt werden. Nichtmonetäre Faktoren wie z. B. Verlust des guten Rufs sind ebenfalls zu berücksichtigen.

Einige Maßnahmen in diesem Dokument lassen sich als Leitprinzipien für das Informationssicherheitsmanagement ansehen und sind auf die meisten Organisationen anwendbar. Sie werden im folgenden unter der Überschrift "Ausgangspunkt für Informationssicherheit" ausführlicher erläutert.

## Ausgangspunkt für Informationssicherheit

Eine Reihe von Maßnahmen können als Leitprinzipien angesehen werden, die einen guten Ausgangspunkt für die Implementierung von Informationssicherheit bilden. Sie beruhen entweder auf grundlegenden gesetzlichen Anforderungen oder werden allgemein als beste Praktiken für die Informationssicherheit anerkannt.

Zu den Maßnahmen, die vom gesetzlichen Standpunkt aus gesehen von wesentlicher Bedeutung für eine Organisation sind, gehören:

- a) Rechte zum Schutz des geistigen Eigentums (siehe 12.1.2),
- b) Sicherung organisationseigener Aufzeichnungen (siehe 12.1.3),
- c) Datenschutz und Geheimhaltung persönlicher Informationen (siehe 12.1.4).

Zu den Maßnahmen, die allgemein als beste Praktiken für die Informationssicherheit anerkannt werden, gehören:

- a) Dokument zur Informationssicherheitspolitik (siehe 3.1.1),
- b) Zuweisung der Verantwortung für Informationssicherheit (siehe 4.1.3),
- c) Ausbildung und Schulung in der Informationssicherheit (siehe 6.2.1),
- d) Meldung von Sicherheitsvorfällen (siehe 6.3.1),
- e) Management des kontinuierlichen Geschäftsbetriebs (siehe 11.1).

Diese Maßnahmen sind auf die meisten Organisationen und Umgebungen anwendbar: Obwohl alle Maßnahmen in diesem Dokument wichtig sind, wird daraufhingewiesen, daß die Bedeutung einer Maßnahme in Abhängigkeit von den spezifischen Risiken festgelegt werden sollte, denen sich eine Organisation gegenüber sieht. Auch wenn der oben dargestellte Ansatz als guter Ausgangspunkt angesehen werden kann, reicht er nicht aus, um eine auf einer Risikoanalyse beruhende Auswahl von Maßnahmen zu ersetzen.

## Entscheidende Erfolgsfaktoren

Die Erfahrung hat gezeigt, dass die folgenden Faktoren oft entscheidend für die erfolgreiche Implementierung von Informationssicherheit innerhalb einer Organisation sind:

- a) Sicherheitspolitik, -ziele und -aktivitäten als Ausdruck der Geschäftsziele;
- b) Implementierung von Sicherheit in Übereinstimmung mit der Organisationskultur;
- c) offenkundige Unterstützung und Engagement seitens der Geschäftsführung;
- d) eingehende Kenntnis der Sicherheitsanforderungen, der Risikoanalyse und des Risikomanagements;
- e) effektives Marketing von Sicherheit gegenüber allen Managern und Mitarbeitern;
- f) Verteilung von Richtlinien über Informationssicherheitspolitik und Normen an alle Angestellte und Auftragnehmer;
- g) entsprechende Ausbildungs- und Schulungsangebote;
- h) umfassendes und ausgewogenes Maßsystem zur Leistungsbeurteilung beim Informationssicherheitsmanagement und zum Feedback von Verbesserungsvorschlägen.

## Entwicklung Ihrer eigenen Richtlinien

Dieser Leitfaden kann als Ausgangspunkt für die Entwicklung organisationsspezifischer Richtlinien angesehen werden. Unter Umständen sind nicht alle Richtlinien und Maßnahmen in diesem Leitfaden anwendbar. Darüber hinaus können zusätzliche Maßnahmen erforderlich sein, die nicht in diesem Dokument enthalten sind. Beim Auftreten eines solchen Falles kann es sich als nützlich erweisen, Querverweise beizubehalten, die eine Prüfung der Normerfüllung durch Auditoren und Geschäftspartner erleichtern.

## 1 Anwendungsbereich

Dieser Teil der Norm BS 7799 gibt Empfehlungen für das Informationssicherheitsmanagement zur Anwendung durch diejenigen Personen, die in einer Organisation für die Einführung, Implementierung und Erhaltung der Sicherheit verantwortlich sind. Er soll eine gemeinsame Basis zur Entwicklung von organisationsbezogenen Sicherheitsnormen und effektiven Sicherheitsmanagementpraktiken bilden und Vertrauen in die Geschäftsbeziehungen zwischen Organisationen herstellen.

## 2 Begriffe und Definitionen

Im Rahmen dieses Dokuments gelten die folgenden Definitionen:

### 2.1 Informationssicherheit

Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Hinweis: Vertraulichkeit wird definiert als Gewährleistung des Zugangs<sup>2</sup> zu Informationen nur für Zugangsberechtigte.

Integrität wird definiert als Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden. Verfügbarkeit wird definiert als Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer.

### 2.2 Risikoanalyse

Analyse von Bedrohungen, Auswirkungen und Schwachstellen bei Informationen und Geräten zur Informationsverarbeitung und die Wahrscheinlichkeit des Auftretens dieser Risiken.

### 2.3 Risikomanagement

Prozess der kostenmäßig vertretbaren Identifizierung, Beschränkung und Minimierung bzw. Elimination von Sicherheitsrisiken, die Informationssysteme beeinträchtigen können.

## 3 Sicherheitspolitik

### 3.1 Informationssicherheitspolitik

Ziel: Richtungsvorgabe für und Unterstützung durch die Geschäftsrührung bei der Informationssicherheit. Die Geschäftsführung sollte bei der Informationssicherheitspolitik eine klare Richtung vorgeben und Unterstützung und Engagement durch organisationsweite Veröffentlichung und Aufrechterhaltung dieser Politik zeigen.

#### 3.1.1 Dokument zur Informationssicherheitspolitik

Die Geschäftsführung sollte ein Dokument zur Informationssicherheitspolitik genehmigen, veröffentlichen und nach Bedarf an alle Mitarbeiter verteilen. Es sollte das Engagement der

---

<sup>2</sup> Zugang beschreibt hier und im folgenden sowohl den physischen wie auch den logischen Zugang.

Geschäftsführung aufzeigen und den Ansatz der Organisation für das Management der Informationssicherheit darstellen. Es sollten mindestens folgende Richtlinien enthalten sein:

- a) Definition von Informationssicherheit, all ihrer Ziele und ihr Anwendungsbereich, sowie die Wichtigkeit von Sicherheit als Mechanismus, der die gemeinsame Nutzung von Informationen ermöglicht (siehe Einleitung);
- b) Absichtserklärung des Managements, Ziele und Prinzipien der Informationssicherheit zu unterstützen;
- c) kurze Erläuterung der Sicherheitspolitiken, Prinzipien, Normen und Konformitätsanforderungen, die von besonderer Bedeutung für die Organisation sind, z. B.:
  - 1) Einhaltung der gesetzlichen und vertraglichen Anforderungen,
  - 2) Anforderungen an die Sicherheitsausbildung,
  - 3) Vermeidung und Erkennung von Viren und anderer bösartiger Software,
  - 4) Management zur Aufrechterhaltung des Geschäftsbetriebs,
  - 5) Konsequenzen bei Verstößen gegen die Sicherheitspolitik;
- d) Definition allgemeiner und spezifischer Zuständigkeiten für sämtliche Aspekte des Informationssicherheitsmanagements, einschließlich der Meldung von Sicherheitsvorfällen;
- e) Verweise auf Dokumentation, die die Politik unterstützt, z. B. ausführlichere Sicherheitspolitiken und -verfahren für spezifische Informationssysteme oder von den Benutzern einzuhaltende Sicherheitsregeln.

Diese Politik sollte in einer für die Zielgruppe relevanten, zugänglichen und verständlichen Form an alle Benutzer in der Organisation verteilt werden.

### **3.1.2 Überprüfung und Bewertung**

Die Politik sollte von einem bestimmten Mitarbeiter verwaltet werden, der für ihre Aufrechterhaltung und Überprüfung gemäß eines definierten Überprüfungsprozesses verantwortlich ist. Dieser Prozess sollte sicherstellen, dass eine Überprüfung als Reaktion auf Änderungen vorgenommen wird, die die Grundlage der ursprünglichen Risikoanalyse beeinflussen, z. B. erhebliche Sicherheitsvorfälle, neue Schwachstellen oder Änderungen in der organisationsbezogenen oder technischen Infrastruktur. Folgende Punkte sollten in regelmäßig wiederkehrenden Abständen geprüft werden:

- a) Effektivität der Politik, nachgewiesen durch Art, Anzahl und Auswirkung der registrierten Sicherheitsvorfälle;
- b) Kosten und Auswirkungen der Maßnahmen auf die Effizienz des Unternehmens,
- c) Folgen von technischen Änderungen.

## 4 Organisation der Sicherheit

### 4.1 Infrastruktur der Informationssicherheit

Ziel: Verwaltung von Informationssicherheit innerhalb der Organisation.

Ein Rahmen für die Verwaltung sollte geschaffen werden, um die Implementierung von Informationssicherheit innerhalb der Organisation einzuführen und zu kontrollieren.

Unter der Leitung der Geschäftsführung sollten geeignete Managementforen gebildet werden, um die Informationssicherheitspolitik zu genehmigen, Rollen in der Sicherheit zu verteilen und die Implementierung von Sicherheit organisationsweit zu koordinieren. Bei Bedarf sollte eine fachliche Beratungsstelle für Informationssicherheit eingerichtet und innerhalb der Organisation verfügbar gemacht werden. Kontakte zu externen Sicherheitsfachkräften sollten hergestellt werden, um mit industriellen Trends Schritt zu halten. Normen und Beurteilungsmethoden zu überwachen sowie geeignete Anlaufstellen zur Behandlung von Sicherheitsvorfällen zu schaffen. Eine interdisziplinäre Vorgehensweise bei der Informationssicherheit sollte gefördert werden, z. B. Mitwirkung und Zusammenarbeit von Managern, Benutzern, Systemadministratoren, Anwendungsdesignern, Auditoren und Sicherheitspersonal sowie Einbeziehung von Fachleuten aus Bereichen wie z. B. Versicherung und Risikomanagement.

#### 4.1.1 Managementforum für Informationssicherheit

Informationssicherheit ist eine Geschäftsverantwortung, die von allen Mitgliedern des Management-Teams geteilt wird. Es sollte deshalb erwogen werden, ein Managementforum ins Leben zu rufen, das eine klare Ausrichtung und sichtbare Unterstützung des Managements für Sicherheitsinitiativen gewährleistet. Dieses Forum sollte die Sicherheit innerhalb der Organisation durch entsprechendes Engagement und angemessene Bereitstellung von Ressourcen fördern. Das Forum kann Teil eines bereits bestehenden Managementorgans sein. Ein Forum hat normalerweise folgende Aufgaben:

- a) Überprüfung und Genehmigung der Informationssicherheitspolitik und der Gesamtverantwortung,
- b) Überwachung signifikanter Änderungen, die Informationswerte wichtigen Bedrohungen aussetzen könnten,
- c) Überprüfung und Überwachung von Sicherheitsvorfällen.
- d) Genehmigung wichtiger Initiativen zur Verstärkung der Informationssicherheit.

Einem Manager sollte die Verantwortung für alle sicherheitsbezogenen Aktivitäten übertragen werden.

#### 4.1.2 Koordination der Informationssicherheit

In einer großen Organisation könnte ein Forum mit übergreifender Funktion erforderlich sein, das sich aus Vertretern des Managements aus wichtigen Teilen der Organisation zusammensetzt, um die Implementierung von Maßnahmen für die Informationssicherheit zu koordinieren. Typische Aufgaben eines derartigen Forums sind:

- a) organisationsweite Vereinbarung bestimmter Rollen und Zuständigkeiten für die Informationssicherheit;
- b) Vereinbarung spezifischer Methoden und Prozesse für die Informationssicherheit, z. B. Risikoanalyse, System der Einstufung von Informationen;
- c) Zustimmung und Unterstützung organisationsweiter Initiativen für die Informationssicherheit, z. B. Programm zur Förderung des Sicherheitsbewusstseins;
- d) Gewähr von Sicherheit als Teil des Planungsprozesses für Informationen und deren Verarbeitung;
- e) Beurteilung der Verhältnismäßigkeit und Koordination der Implementierung spezifischer Maßnahmen für Informationssicherheit bei neuen Systemen oder Diensten;
- f) Überprüfung von Sicherheitsvorfällen;
- g) organisationsweite Förderung der Sichtbarkeit der Unterstützung der Geschäftsführung für Informationssicherheit.

#### **4.1.3 Zuweisung der Zuständigkeiten für Informationssicherheit**

Zuständigkeiten für den Schutz einzelner Werte und für die Durchführung spezifischer Sicherheitsprozesse sollten klar definiert sein.

Die Informationssicherheitspolitik (siehe Punkt 3) sollte allgemeine Richtlinien für die Zuweisung von Zuständigkeiten für und Rollen in der Sicherheit und innerhalb der Organisation enthalten. Diese sollte im Bedarfsfall durch ausführlichere Leitlinien für spezifische Standorte, Systeme oder Dienste ergänzt werden. Ortsspezifische Zuständigkeiten für einzelne Sach- und Informationswerte und Sicherheitsprozesse, wie z. B. Planung zur Aufrechterhaltung des Geschäftsbetriebs, sollten klar definiert sein.

In vielen Organisationen wird ein Informationssicherheitsmanager ernannt, der die Gesamtverantwortung für die Entwicklung und Implementierung von Sicherheit übernimmt und die Unterstützung der Identifizierung von Maßnahmen gewährleistet. Allerdings verbleibt die Verantwortung für die Bereitstellung von Ressourcen und Implementierung der Maßnahmen häufig bei dem jeweiligen Manager. Eine verbreitete Vorgehensweise ist die Ernennung eines Eigentümers für jeden Informationswert, der für dessen tägliche Sicherheit verantwortlich ist.

Eigentümer von Informationswerten können ihre Sicherheitszuständigkeit an einzelne Manager oder Dienstleister delegieren. Trotzdem verbleibt die letzte Verantwortung für die Sicherheit des Werts beim Eigentümer, der in der Lage sein sollte, festzustellen, ob die übertragene Verantwortung ordnungsgemäß ausgeübt wurde.

Es ist wichtig, dass die Verantwortungsbereiche jedes Managers klar definiert werden. Dabei handelt es sich vor allem um folgende Punkte:

- a) die verschiedenen Werte und Sicherheitsprozesse, die mit jedem einzelnen System verknüpft sind, sollten identifiziert und klar definiert werden;
- b) der für den jeweiligen Wert oder Sicherheitsprozess verantwortliche Manager sollte ernannt, und die Einzelheiten dieser Zuständigkeit sollten dokumentiert werden;
- c) Berechtigungsebenen sollten klar definiert und dokumentiert werden.

#### 4.1.4 Berechtigungsprozeß für Geräte zur Informationsverarbeitung

Für neue Geräte zur Informationsverarbeitung sollte ein Prozess zur Gewährleistung der Berechtigung des Managements geschaffen werden.

Folgende Punkte sollten berücksichtigt werden:

- a) für neue Geräte sollte es eine entsprechende Genehmigung der Benutzerverwaltung geben, die deren Zweck und Nutzen festlegt; es sollte auch eine Genehmigung von dem Manager eingeholt werden, dem die Wartung der lokalen Informationssystem-sicherheitsumgebung anvertraut ist, um die Erfüllung aller relevanten Sicherheitspolitiken und -anforderungen sicherzustellen;
- b) bei Bedarf sollte die Hardware und Software geprüft werden, um die Kompatibilität mit den übrigen Systemkomponenten sicherzustellen;  
Hinweis: Für bestimmte Verbindungen kann eine Bauartzulassung erforderlich sein.
- c) die Verwendung von privaten Verarbeitungsgeräten zur Verarbeitung von geschäftlichen Informationen und alle dafür notwendigen Maßnahmen sollten genehmigt werden;
- d) die Verwendung von privaten Verarbeitungsgeräte am Arbeitsplatz kann neue Schwachstellen verursachen und sollte deswegen beurteilt und genehmigt werden.

Diese Maßnahmen sind besonders in einer vernetzten Umgebung wichtig.

#### 4.1.5 Fachliche Informationssicherheitsberatung

Fachliche Sicherheitsberatung wird wahrscheinlich von vielen Organisationen benötigt. Idealerweise sollte diese von einem erfahrenen hausinternen Informationssicherheitsberater angeboten werden. Nicht alle Organisationen benötigen einen fest angestellten Fachberater. In so einem Fall empfiehlt es sich, eine Person für die Koordination der organisationsinternen Kenntnisse und Erfahrungen zu bestimmen, damit Einheitlichkeit und Unterstützung bei sicherheitsspezifischen Entscheidungen gewährleistet ist. Diese Person sollte auch Zugang zu geeigneten externen Beratern haben, die zusätzlichen fachlichen Rat geben können.

Informationssicherheitsberatern oder vergleichbaren Ansprechpartnern sollte die Aufgabe übertragen werden, fachlichen Rat zu allen Aspekten der Informationssicherheit zu geben, wobei entweder die eigene oder externe Sachkenntnis zur Anwendung kommt. Die Qualität ihrer Analyse von Sicherheitsbedrohungen und ihrer Beratung bezüglich Maßnahmen entscheidet über die Effektivität des Informationssicherheitsprogramms der Organisation. Zur Erzielung höchster Effektivität und Wirkung sollte ihnen organisationsweit direkter Zugang zum Management ermöglicht werden.

Der Informationssicherheitsberater oder der entsprechende Ansprechpartner sollte so früh wie möglich nach einem vermuteten Sicherheitsvorfall oder -verstoß zu Rate gezogen werden, um eine Quelle fachkundiger Hilfe oder Untersuchungsmittel verfügbar zu machen. Obwohl die meisten internen Sicherheitsuntersuchungen normalerweise unter Aufsicht des Managements vorgenommen werden, kann der Informationssicherheitsberater zur Beratung, Leitung oder Durchführung dieser Untersuchung hinzugezogen werden.

#### **4.1.6 Kooperation zwischen Organisationen**

Es sollten entsprechende Kontakte zu Vollzugs- und Aufsichtsbehörden, Informationsdiensteanbietern und Telekommunikationsunternehmen bestehen, damit bei einem Sicherheitsvorfall eine schnelle Umsetzung entsprechender Maßnahmen möglich ist und spezifische Unterstützung gegeben werden kann. Eine Mitgliedschaft in Gruppen, die sich mit sicherheitsbezogenen Fragen befassen, und in entsprechenden industriespezifischen Foren sollte ebenso in Betracht gezogen werden.

Der Austausch von Sicherheitsinformationen sollte begrenzt werden, damit sichergestellt wird, dass vertrauliche Informationen über die Organisation nicht an unberechtigte Personen weitergegeben werden.

#### **4.1.7 Unabhängige Überprüfung von Informationssicherheit**

Das Dokument zur Informationssicherheitspolitik (siehe 3.1.1) zeigt die Politik und die Verantwortlichkeiten für die Informationssicherheit auf. Ihre Implementierung sollte aus unabhängiger Sicht überprüft werden, um eine entsprechende Berücksichtigung der Politik in den organisationseigenen Praktiken und ihre Durchführbarkeit und Effektivität sicherzustellen (siehe 12.2).

Eine derartige Überprüfung sollte durch eine interne Auditfunktion, eine unabhängige Führungskraft oder eine externe Organisation durchgeführt werden, deren Spezialgebiet solche Revisionen sind und wo diese Experten die entsprechenden Fähigkeiten und Erfahrungen besitzen.

## **4.2 Sicherheit bei dem Zugang durch Fremdunternehmen**

Ziel: Erhaltung der Sicherheit organisationseigener Geräte zur Informationsverarbeitung und Informationswerte, zu denen Fremdunternehmen Zugang haben.

Der Zugang zu den Informationsverarbeitungsgeräten der Organisation durch Fremdunternehmen sollte überwacht werden.

Wo ein Zugang eines derartigen Fremdunternehmens geschäftlich erforderlich ist, sollte eine Risikoanalyse vorgenommen werden, um die Auswirkungen auf die Sicherheit und die Anforderungen an die Maßnahmen zu ermitteln. Maßnahmen sollten vertraglich mit dem Fremdunternehmen vereinbart und definiert werden.

Ein derartiger Zugang von Fremdunternehmen kann andere Teilnehmer einschließen. Verträge, die den Zugang von Fremdunternehmen regeln, sollten die Ermächtigung zur Bestimmung anderer berechtigter Teilnehmer sowie die Bedingungen für ihren Zugang enthalten.

Diese Norm kann als Grundlage für derartige Verträge und bei Überlegungen zum Outsourcing von Tätigkeiten der Informationsverarbeitung verwendet werden.

## 4.2.1 Identifizierung der Risiken bei dem Zugang von Fremdunternehmen

### 4.2.1.1 Zugriffsarten

Die Art des Zugangs, der einem Fremdunternehmen eingeräumt wird, ist von besonderer Bedeutung. Beispielsweise unterscheiden sich die Risiken bei einem Zugang über eine Netzverbindung von denen bei einem physischen Zugang. Zugriffsarten, die in Betracht gezogen werden sollten, sind:

- a) Physischer Zugang, z. B. zu Büro- und Computerräumen, Aktenschränken;
- b) logischer Zugang, z. B. zu den Datenbanken und Informationssystemen einer Organisation.

### 4.2.1.2 Gründe für den Zugang

Fremdunternehmen kann aus verschiedenen Gründen Zugang gewährt werden. Beispielsweise kann es sich um Fremdunternehmen handeln, die einen Dienst für die Organisation erbringen, sich nicht am Standort der Organisation befinden und denen folgender physischer und logischer Zugang gegeben wird:

- a) Mitarbeiter aus dem Hardware- und Software-Support, die einen Zugang auf Systemebene oder zu grundlegenden Anwendungsfunktionen benötigen.
- b) Handels- oder Joint-Venture-Partner, die Informationen austauschen, auf Informationssysteme zugreifen oder Datenbanken gemeinsam nutzen.

Durch unzulängliches Sicherheitsmanagement können Informationen bei dem Zugriff von Fremdunternehmen gefährdet werden. Wo es geschäftlich notwendig ist, sich mit dem Standort eines Fremdunternehmens zu verbinden, sollte eine Risikoanalyse zur Identifizierung etwaiger Anforderungen für spezifische Maßnahmen durchgeführt werden. Dabei sollten die benötigte Zugriffsart, der Wert der Informationen sowie die vom Fremdunternehmen verwendeten Maßnahmen und die Konsequenzen des Zugriffs für die Sicherheit der Informationen der Organisation berücksichtigt werden.

### 4.2.1.3 Auftragnehmer am Standort der Organisation

Fremdunternehmen, die sich vertragsgemäß für einen bestimmten Zeitraum am Standort der Organisation befinden, können ebenfalls Schwachstellen für die Sicherheit darstellen. Beispiele für Fremdunternehmen am Standort der Organisation:

- a) mit Wartung und Support von Hardware und Software beauftragte Mitarbeiter;
- b) Reinigungs-, Kantinen- und Sicherheitspersonal und andere Mitarbeiter für ausgelagerte Dienstleistungen;
- c) Praktikanten und andere vorübergehend beschäftigte Mitarbeiter;
- d) Berater.

Man sollte unbedingt wissen, welche Maßnahmen benötigt werden, um den Zugang von Fremdunternehmen zu Informationsverarbeitungsgeräten zu regeln. Generell sollten alle Sicherheitsanforderungen, die sich aus dem Zugang von Fremdunternehmen oder durch

interne Maßnahmen ergeben, im Vertrag mit dem Fremdunternehmen enthalten sein (siehe auch 4.2.2). Sollte sich eine besondere Notwendigkeit für die vertrauliche Behandlung von Informationen ergeben, können beispielsweise auch Vertraulichkeitsvereinbarungen verwendet werden (siehe 6.1.3). Fremdunternehmen sollte erst dann Zugang zu Informationen und Informationsverarbeitungsgeräten eingeräumt werden, wenn die entsprechenden Maßnahmen implementiert worden sind und ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.

#### 4.2.2 Sicherheitsanforderungen in Verträgen mit Fremdunternehmen

Vereinbarungen, die den Zugang von Fremdunternehmen zu organisationseigenen Informationsverarbeitungsgeräten regeln, sollten auf einem formalen Vertrag beruhen, der sämtliche erforderlichen Sicherheitsanforderungen enthält oder sich auf sie bezieht, um die Erfüllung der Sicherheitspolitiken und -normen der Organisation zu gewährleisten. Der Vertrag sollte sicherstellen, dass es keine Missverständnisse zwischen der Organisation und dem Fremdunternehmen gibt. Organisationen sollten die Haftungsfrage mit ihrem Lieferanten regeln. Die Aufnahme der folgenden Bedingungen in den Vertrag sollte erwogen werden:

- a) allgemeine Politik zur Informationssicherheit;
- b) Schutz der Werte, einschließlich:
  - 1) Verfahren zum Schutz organisationseigener Werte, einschließlich Informationen und Software;
  - 2) Verfahren zur Bestimmung, ob eine Kompromittierung von Werten stattgefunden hat, z. B. bei Verlust oder Veränderung von Daten;
  - 3) Maßnahmen zur Sicherstellung der Rückgabe oder Vernichtung von Informationen und Werten am Ende eines Vertrags oder zu einem vereinbarten Zeitpunkt während des Vertrags;
  - 4) Integrität und Verfügbarkeit;
  - 5) Beschränkungen bei der Vervielfältigung und Offenlegung von Informationen;
- c) Vorhandensein einer Beschreibung jedes Dienstes;
- d) Zielvorgabe für das Niveau des zu erbringenden Dienstes und nicht akzeptable Leistungserbringung;
- e) Vorkehrungen für die bedarfsorientierte Überlassung von Mitarbeitern;
- f) jeweilige Verpflichtungen der Parteien bezüglich der Vereinbarung.
- g) Verantwortlichkeiten bezüglich der gesetzlichen Bestimmungen, z. B. Datenschutzgesetze, insbesondere unter Berücksichtigung der unterschiedlichen nationalen Rechtssysteme, wenn dem Vertrag eine Kooperation mit Organisationen in anderen Ländern zugrunde liegt (siehe auch 12.1);
- h) Rechte zum Schutz des geistigen Eigentums und Copyright-Abtretungen (siehe 12.1.2) und Schutz gemeinsamer Arbeitsergebnisse (siehe auch 6.1.3);
- i) Vereinbarung über die Zugriffskontrolle, einschließlich:

- 1) erlaubte Zugriffsmethoden sowie die Kontrolle und Benutzung von Kennungen (wie Benutzer-IDs) und Passwörtern;
  - 2) Berechtigungsprozeß für den Benutzerzugriff und -Privilegien;
  - 3) Anforderung, eine Liste von Einzelpersonen zu führen, die zur Benutzung der zur Verfügung gestellten Dienste berechtigt sind; sie enthält auch eine Beschreibung der Rechte und -Privilegien im Hinblick auf diese Benutzung;
- 
- j) Definition überprüfbarer Leistungskriterien, ihre Überwachung und Meldung;
  - k) Recht, Benutzeraktivitäten zu überwachen und zu widerrufen;
  - l) Recht, vertragliche Verantwortlichkeiten zu prüfen bzw. diese Audits durch ein Fremdunternehmen ausführen zu lassen;
  - m) Einrichtung eines Eskalationsprozesses zur Problemlösung oder ggf. auch die Berücksichtigung von Notfallplänen in entsprechenden Fällen;
  - n) Verantwortlichkeiten in bezug auf Installierung und Wartung von Hardware und Software;
  - o) klare Meldungsstruktur und vereinbarte Meldeformate;
  - p) klarer und festgelegter Prozeß für das Management von Veränderungen;
  - q) alle erforderlichen physischen Schutzmaßnahmen und Mechanismen, die sicherstellen, dass diese Maßnahmen eingehalten werden;
  - r) Benutzer- und Administratorschulung in Methoden, Verfahren und Sicherheit;
  - s) Maßnahmen, die einen Schutz vor bösartiger Software (siehe 8.3) sicherstellen;
  - t) Vereinbarungen für die Meldung, Benachrichtigung und Untersuchung von Sicherheitsvorfällen und Sicherheitsverstößen;
  - u) Einbeziehung von Fremdunternehmen mit Unterlieferanten.

### **4.3 Outsourcing**

Ziel: Aufrechterhaltung der Sicherheit der Informationen, wenn die Verantwortung für die Informationsverarbeitung an eine andere Organisation übertragen wurde.

Outsourcing-Vereinbarungen sollten die Risiken, Sicherheitsmaßnahmen und -verfahren für Informationssysteme, Netzwerke und/oder Desktop-Umgebungen im Vertrag zwischen den Partnern berücksichtigen.

#### **4.3.1 Sicherheitsanforderungen in Outsourcing-Verträgen**

Die Sicherheitsanforderungen einer Organisation, die das Management und die Kontrolle für alle oder einige Informationssysteme, -netzwerke und/oder Desktop-Umgebungen auslagert, sollten in einem zwischen den Parteien vereinbarten Vertrag behandelt werden.

Beispielsweise sollte dieser Vertrag klären:

- a) wie gesetzliche Anforderungen zu erfüllen sind, z. B. Datenschutzgesetz;
- b) Vereinbarungen, die sicherstellen, dass sich alle am Outsourcing beteiligten Parteien, einschließlich der Untervertragspartner, ihrer Sicherheitsverantwortlichkeiten bewusst sind;

- c) Aufrechterhaltung und Test der Integrität und der Vertraulichkeit der Geschäftswerte der Organisation;
- d) physische und logische Maßnahmen, um den Zugang zu sensitiven Geschäftsinformationen der Organisation auf berechnigte Benutzer einzuschränken und zu begrenzen;
- e) Aufrechterhaltung der Verfügbarkeit von Diensten im Falle einer Katastrophe;
- f) Stufen der bereitzustellenden physischen Sicherheit für die ausgelagerten Geräte;
- g) Recht zum Audit.

Die Bedingungen, die in der Liste unter 4.2.2 aufgeführt sind, sollten ebenfalls als Teil dieses Vertrags angesehen werden. Der Vertrag sollte die Erweiterung der Sicherheitsanforderungen und -verfahren zu einem Sicherheitsmanagementplan ermöglichen, der zwischen den zwei Parteien zu vereinbaren ist.

Obwohl sich beim Outsourcing von Verträgen einige komplexe Sicherheitsfragen stellen, könnten die in diesem Leitfadenthaltenen Maßnahmen als Ausgangspunkt für die Abstimmung der Struktur und des Inhalts eines Sicherheitsmanagementplan dienen.

## **5 Einstufung und Kontrolle der Werte**

### **5.1 Zurechenbarkeit für Werte**

Ziel: Aufrechterhaltung eines angemessenen Schutzes für organisationseigene Werte.

Für alle wichtigen Informationswerte sollte eine Zurechenbarkeit bestehen, und eine für sie zuständige Person ernannt werden.

Die Zurechenbarkeit für Werte trägt dazu bei, dass angemessener Schutz aufrechterhalten wird. Neben der Benennung von zuständigen Personen für alle wichtigen Werte sollte ihnen auch die Verantwortung für die Aufrechterhaltung geeigneter Maßnahmen zugewiesen werden. Die Verantwortlichkeit für die Implementierung von Maßnahmen kann auch delegiert werden. Die Zurechenbarkeit sollte bei der ernannten zuständigen Person des Werts verbleiben.

#### **5.1.1 Inventar der Werte**

Inventare von Werten tragen dazu bei, dass ein effektiver Schutz von Werten gewährleistet ist. Sie können auch für andere Geschäftszwecke erforderlich sein, z.B. aus Gesundheits- und Sicherheitsgründen, versicherungstechnischen oder finanziellen Gründen (Werte Verwaltung). Der Prozess der Erstellung eines Inventars von Werten ist ein wichtiger Aspekt des Risikomanagements. Eine Organisation muss in der Lage sein, ihre Werte und deren relative Bewertung und ihre Bedeutung dieser Werte feststellen zu können. Auf der Grundlage dieser Informationen kann eine Organisation ein Schutzniveau gewährleisten, das der Bewertung und der Bedeutung der Werte angemessen ist. Ein Inventar der wichtigen Werte, die mit jedem Informationssystem verbunden sind, sollte erstellt und geführt werden. Jeder Wert sollte klar gekennzeichnet und die dafür zuständige Person und seine Sicherheitseinstufung (siehe 5.2), zusammen mit seinem aktuellen Standort (vor allem von Bedeutung, wenn eine Wiederherstellung bei Verlust oder Beschädigung versucht wird) vereinbart und dokumentiert sein. Beispiele von Werten in Verbindung mit Informationssystemen sind:

- a) Informationswerte: Datenbanken und Dateien, Systemdokumentation, Benutzerhandbücher, Schulungsunterlagen, Betriebs- oder Supportverfahren, Kontinuitätspläne, Reservevereinbarungen, archivierte Informationen;
- b) Software-Werte: Anwendungssoftware, Systemsoftware, Entwicklungstools und Dienstprogramme;
- c) physische Werte: Computerausstattung (Prozessoren, Monitore, Laptops, Modems), Kommunikationsgeräte (Router, Nebenstellengeräte, Faxgeräte, Anrufbeantworter), Speichermedien (Bänder und Disketten), andere technische Ausstattung (Netzgeräte, Klimageräte), Möbel, Räumlichkeiten;
- d) Dienste: Rechner- und Kommunikationsdienste, allgemeine Dienste (z.B. Heizung, Licht, Strom, Klimatechnik).

## **5.2 Einstufung von Informationen**

Ziel: Sicherstellung eines angemessenen Schutzes für Informationswerte.

Informationen sollten eingestuft werden, um Bedarf, Prioritäten und Umfang des Schutzes angeben zu können.

Bei Informationen kann das Niveau der Sensitivität und Wichtigkeit unterschiedlich sein. Manche Elemente können einen zusätzlichen Sicherheitsschutz oder eine besondere Behandlung erfordern. Zur Definition eines angemessenen Schutzes und zur Vermittlung der Notwendigkeit besonderer Behandlungsmaßnahmen sollte ein System für die Einstufung von Informationen verwendet werden.

### **5.2.1 Richtlinien für die Einstufung**

Einstufungen und damit verbundene Schutzmaßnahmen für Informationen sollten die Geschäftsanforderungen für die gemeinsame oder eingeschränkte Nutzung von Informationen berücksichtigen sowie die mit solchen Anforderungen verbundenen geschäftlichen Folgen, z.B. nicht genehmigter Zugang oder Beeinträchtigung von Informationen. Die einer Information zugewiesene Einstufung ist im allgemeinen eine einfache Methode, um die Behandlung und den Schutz für diese Information festzulegen. Informationen und Ausgaben von Systemen, die eingestufte Daten behandeln, sollten hinsichtlich ihres Werts und ihrer Sensitivität für die Organisation gekennzeichnet werden. Es kann auch angebracht sein, Informationen hinsichtlich ihrer Wichtigkeit für die Organisation, z.B. in bezug auf ihre Integrität und Verfügbarkeit, zu kennzeichnen.

Nach einem bestimmten Zeitraum, z.B. nach Veröffentlichung der Informationen, sind die Informationen häufig nicht mehr sensitiv oder wichtig. Dies sollte berücksichtigt werden, da eine zu hohe Einstufung zu unnötigen zusätzlichen Geschäftsausgaben führen kann. Einstufungsrichtlinien sollten die Tatsache vorwegnehmen bzw. berücksichtigen, dass die Einstufung bei bestimmten Informationen nicht unbedingt für immer festgelegt ist, sondern sich gemäß einer vorher festgelegten Politik (siehe 9. 1) ändern kann.

Die Anzahl der Einstufungskategorien und die Vorteile, die aus ihrer Nutzung erwachsen, sollten gründlich überlegt werden. Übermäßig komplexe Einteilungen könnten sich in der Verwendung als schwerfällig, unwirtschaftlich oder unpraktisch erweisen. Einstufungsbezeichnungen auf Dokumenten anderer Organisationen sollten mit Vorsicht interpretiert werden, da diese Organisationen andere

Definitionen für dieselbe oder eine ähnlich lautende Bezeichnung haben könnten.

Die Verantwortung für die Bestimmung der Einstufung von Informationen, z.B. eines Dokuments, eines Datensatzes, einer Datei oder Diskette sollte wie auch die periodische Überprüfung der Einstufung dem Urheber oder der ernannten zuständigen Person der Information überlassen bleiben.

## **5.2.2 Kennzeichnung und Behandlung von Informationen**

Es ist wichtig, dass entsprechende Verfahren für die Kennzeichnung und Behandlung von Informationen gemäß der von der Organisation angewendeten Einstufung definiert werden. Diese Verfahren müssen die Informationswerte in physischer und elektronischer Form erfassen. Für jeden Grad der Einstufung sollten Behandlungsverfahren definiert werden, in denen die folgenden Arten von Aktivitäten in der Informationsverarbeitung enthalten sind:

- a) Vervielfältigung;
- b) Speicherung;
- c) Übertragung auf dem Postweg, per Fax oder E-Mail;
- d) Übertragung durch das gesprochene Wort, einschließlich Mobiltelefon, Voice Mail, Anrufbeantworter;
- e) Vernichtung.

Ausgaben von Systemen, die als sensitiv oder wichtig eingestufte Informationen enthalten, sollten über eine entsprechende Kennzeichnung (in der Ausgabe) verfügen. Die Kennzeichnung sollte die Einstufung gemäß der in 5.2.1 aufgestellten Regeln widerspiegeln. Beachtet werden sollten dabei gedruckte Berichte, Bildschirmdisplays, magnetische Datenträger (Bänder, Disketten, CD-ROM, Kassetten), elektronische Nachrichten und Dateiübertragung.

Physische Beschriftungen sind normalerweise die geeignetste Form der Kennzeichnung. Einige Informationsbestandteile wie z.B. Dokumente in elektronischer Form können jedoch nicht physisch beschriftet werden, weshalb eine elektronische Form der Kennzeichnung verwendet werden muss.

## **6 Personelle Sicherheit**

### **6.1 Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen**

Ziel: Reduzierung der Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch der Einrichtungen.

Sicherheitsverantwortlichkeiten sollten bei der Einstellung angesprochen, in Verträge aufgenommen und während der Beschäftigung der Person überprüft werden.

Stellenbewerber sollten vor allem im Hinblick auf sensitive Aufgaben einer angemessenen Überprüfung unterzogen werden (siehe 6.1.2). Alle Benutzer von Geräten zur Informationsverarbeitung, d.h. die eigenen Angestellten und die Mitarbeiter eines Fremdenunternehmens, sollten eine Vertraulichkeitsvereinbarung unterschreiben.

### 6.1.1 Einbeziehung von Sicherheit in Arbeitsverantwortlichkeiten

Sicherheitsrollen und -Verantwortlichkeiten, die in der Informationssicherheitspolitik der Organisation festgelegt sind (siehe 3.1.1), sollten angemessen dokumentiert sein. Sie sollten sämtliche allgemeine Verantwortlichkeiten für die Implementierung und Wartung der Sicherheitspolitik enthalten. Hierzu gehören auch spezifische Verantwortlichkeiten für den Schutz bestimmter Werte oder für die Ausführung bestimmter Sicherheitsprozesse oder -aktivitäten.

### 6.1.2 Überprüfung der Mitarbeiter und Personalpolitik

Überprüfungen von festangestellten Mitarbeitern sollten zum Zeitpunkt der Bewerbung ausgeführt werden. Diese Prüfung sollte sich auf folgende Bereiche erstrecken:

- a) Vorhandensein befriedigender Referenzen, z.B. eine Referenz geschäftlicher und eine persönlicher Natur;
- b) Überprüfung (auf Vollständigkeit und Genauigkeit) des Lebenslaufs des Bewerbers;
- c) Bestätigung akademischer und beruflicher Qualifikationen;
- d) unabhängige Identitätsprüfung (Reisepass oder ähnliches Dokument).

Darüber hinaus sollte die Organisation in den Fällen, in denen die Person Zugang zu Geräten für die Informationsverarbeitung hat, und insbesondere dann, wenn diese sensitive Informationen, z.B. finanzielle Informationen oder sehr vertrauliche Informationen, enthalten, eine Bonitätsprüfung durchführen. Dies sollte für Ersteinstellung oder Beförderung gelten. Bei Mitarbeitern, die Positionen mit erheblicher Entscheidungsgewalt bekleiden, sollte diese Prüfung in regelmäßigen Abständen wiederholt werden.

Für Auftragnehmer und vorübergehende beschäftigte Mitarbeiter sollte ein vergleichbarer Überprüfungsprozess durchgeführt werden. In den Fällen, in denen diese Mitarbeiter durch eine Agentur bereitgestellt werden, sollten in dem Vertrag die Verantwortlichkeiten der Agentur für die Überprüfung klar festgelegt werden. Außerdem sollten Benachrichtigungsverfahren festgelegt werden für den Fall, dass die Überprüfung noch nicht abgeschlossen wurde oder die Ergebnisse Anlass zu Bedenken oder Besorgnis geben.

Bei neuen und unerfahrenen Mitarbeitern, die über eine Zugangsberechtigung für sensitive Systeme verfügen, sollte das Management festlegen, welche Art von Aufsicht erforderlich ist. Die Tätigkeit aller Mitarbeiter sollte in regelmäßigen Abständen einem Prüflings- und Genehmigungsverfahren durch einen leitenden Mitarbeiter unterworfen sein.

Die Führungskräfte sollten sich dessen bewusst sein, dass die persönlichen Umstände ihrer Mitarbeiter deren Arbeit beeinflussen könnten. Persönliche oder finanzielle Probleme, Änderungen im Verhalten oder in der Lebensführung, wiederholtes Fernbleiben von der Arbeit und Zeichen von Stress oder Depression können zu Betrug, Diebstahl, Fehlen oder anderen sicherheitsrelevanten Folgen führen. Mit diesen Informationen sollte gemäß der entsprechenden Gesetzgebung in der jeweiligen Gerichtsbarkeit verfahren werden.

### **6.1.3 Vertraulichkeitsvereinbarungen**

Vertraulichkeits- oder Nichtoffenlegungsvereinbarungen weisen daraufhin, dass Informationen sensitiv, vertraulich oder geheim sind. Angestellte sollten normalerweise eine derartige Vereinbarung als Teil ihrer Anstellungsbedingungen unterschreiben.

Vorübergehend beschäftigte Mitarbeiter von Agenturen und Benutzer von Fremdunternehmen, die noch nicht durch einen bestehenden Vertrag (mit der Vertraulichkeitsvereinbarung) verpflichtet sind, sollten noch vor Gewährung des Zugangs zu den Geräten für die Informationsverarbeitung eine Vertraulichkeitsvereinbarung unterschreiben.

Vertraulichkeitsvereinbarungen sollten überprüft werden, wenn sich die Anstellungsbedingungen oder die Verträge ändern, vor allem dann, wenn Angestellte die Organisation verlassen oder Verträge auslaufen.

### **6.1.4 Anstellungsbedingungen**

Die Anstellungsbedingungen sollten die Verantwortung des Mitarbeiters für die Informationssicherheit beschreiben. Im Bedarfsfall sollten diese Verantwortlichkeiten noch für einen festgelegten Zeitraum nach Ende der Beschäftigung gelten. Die Maßnahmen, die zu ergreifen sind, wenn der Mitarbeiter die Sicherheitsanforderungen missachtet, sollten aufgeführt sein.

Die rechtlichen Verantwortlichkeiten und Rechte des Mitarbeiters, z.B. hinsichtlich der Urheberrechts- und Datenschutzgesetze, sollten klar herausgestellt und in den Anstellungsbedingungen enthalten sein. Die Verantwortung für die Einstufung und das Management der Mitarbeiterdaten sollten ebenfalls enthalten sein. Im Bedarfsfall sollten die Anstellungsbedingungen angeben, dass diese Verantwortlichkeiten auch außerhalb der Geschäftsräume der Organisation und der normalen Arbeitszeit, z.B. bei Telearbeit (siehe auch 7.2.5 und 9.8.1) gelten.

## **6.2 Benutzerschulung**

Ziel: Gewährleistung, dass Benutzer sich der Bedrohungen und Bedenken bezüglich der Informationssicherheit bewusst sind, und dass sie bei ihrer normalen Arbeitsverrichtung über Mittel zur Unterstützung der organisationseigenen Sicherheitspolitik verfügen.

Benutzer sollten in Sicherheitsverfahren und dem richtigen Gebrauch der Geräte zur Informationsverarbeitung geschult werden, um mögliche Sicherheitsrisiken zu verringern.

### **6.2.1 Ausbildung und Schulung in der Informationssicherheit**

Alle Mitarbeiter der Organisation und im Bedarfsfall Benutzer von Fremdfirmen sollten eine entsprechende Schulung und regelmäßig aktualisierte Informationen über die Sicherheitspolitiken und Verfahren der Organisation erhalten. Dazu gehören Sicherheitsanforderungen, rechtliche Verantwortlichkeiten und geschäftliche Maßnahmen sowie Schulung in der ordnungsgemäßen Anwendung von Informationsverarbeitungsgeräten, z.B. korrekte Anmeldung, Benutzung von Softwarepaketen. Dies sollte vor der Gewährung des Zugangs zu Informationen oder Diensten durchgeführt werden.

### 6.3 Verhalten bei Sicherheitsvorfällen und Störungen

Ziel: Schadensbegrenzung bei Sicherheitsvorfällen und Funktionsstörungen, Überwachung derartiger Vorfälle und Erkenntnisgewinn.

Die sicherheitsrelevanten Vorfälle sollten so schnell wie möglich über entsprechende Managementkanäle gemeldet werden.

Alle Angestellten und Auftragnehmer sollten mit den Meldeverfahren für die verschiedenen Arten von Vorfällen (Sicherheitsverstoß, Bedrohung, Schwachstelle oder Störung), die Auswirkungen auf die Sicherheit der organisationseigenen Werte haben könnten, vertraut gemacht werden. Sie sollten verpflichtet sein, alle beobachteten oder vermuteten Vorfälle möglichst schnell an die angegebene Anlaufstelle weiterzuleiten. Die Organisation sollte einen formalen Disziplinarprozess für Angestellte festlegen, die Sicherheitsverstöße begehen. Um eine ordnungsgemäße Bearbeitung eines Vorfalls zu ermöglichen, ist es unter Umständen erforderlich, unmittelbar nach dem Auftreten Beweise zu sammeln (siehe 12.1.7).

#### 6.3.1 Meldung von Sicherheitsvorfällen

Sicherheitsvorfälle sollten so schnell wie möglich über entsprechende Managementkanäle gemeldet werden.

Zusammen mit einem Verfahren zur Vorfallsbehandlung sollte ein formales Meldeverfahren geschaffen werden, das die Maßnahmen festlegt, die bei Erhalt einer Vorfallsmeldung ergriffen werden. Alle Angestellten und Auftragnehmer sind mit dem Meldeverfahren für Sicherheitsvorfälle vertraut zu machen. Außerdem sollte die Verpflichtung bestehen, solche Vorfälle möglichst schnell weiterzuleiten. Durch die Implementierung geeigneter Rückmeldeprozesse sollte sichergestellt sein, dass diejenigen, die einen Vorfall gemeldet haben, nach Behandlung und Klärung des Vorfalls über die Ergebnisse informiert werden. Diese Vorfälle können in Benutzerschulungen (siehe 6.2) als Beispiele dafür dienen, was geschehen könnte, wie bei solchen Vorfällen zu reagieren ist und wie sie zukünftig vermieden werden können (siehe auch 12.1.7).

#### 6.3.2 Meldung von Sicherheitsschwachstellen

Für Benutzer von Informationsdiensten sollte die Verpflichtung bestehen, alle beobachteten oder vermuteten Sicherheitsschwachstellen oder Bedrohungen bezüglich der Systeme oder Dienste aufzuzeichnen und zu melden. Sie sollten diese Beobachtungen möglichst schnell entweder an das Management oder direkt an den Diensteanbieter melden. Benutzer sollten informiert werden, dass sie unter keinen Umständen versuchen sollten, eine vermutete Schwachstelle selbst zu testen. Dies geschieht zu ihrem eigenen Schutz, denn ein Test der Schwachstelle könnte als potentieller Missbrauch des Systems interpretiert werden.

#### 6.3.3 Meldung von Softwarestörungen

Für das Melden von Softwarefunktionsstörungen sind entsprechende Verfahren festzulegen. Folgende Punkte sollten berücksichtigt werden:

- a) Aufzeichnung der Symptome des Problems und aller Bildschirmmeldungen;
- b) nach Möglichkeit Isolierung des Computers und keine weitere Verwendung;  
sofortige Benachrichtigung der entsprechenden Anlaufstelle; ;bei einer Prüfung ist das Gerät vor einem Neustart von allen organisationseigenen Netzen zu trennen;

- keine Verwendung von Disketten mit Daten von diesem Rechner in anderen Rechnern;
- c) sofortige Meldung des Vorfalls an den Informationssicherheitsmanager.

Benutzer sollten nicht ohne eine entsprechende Genehmigung versuchen, die verdächtige Software zu entfernen. Wiederherstellungsmaßnahmen sollten von entsprechend ausgebildeten und erfahrenen Mitarbeitern durchgeführt werden.

#### **6.3.4 Lernen aus Vorfällen**

Es sollten Verfahren vorhanden sein, mit denen Arten, Umfang und Kosten von Vorfällen und Störungen quantitativ erfasst und überwacht werden können. Mit diesen Informationen können wiederkehrende oder schwerwiegende Vorfälle oder Störungen ermittelt werden. Sie können die Notwendigkeit von erweiterten oder zusätzlichen Maßnahmen anzeigen und zur Begrenzung der Häufigkeit, des Schadens und der Kosten bei zukünftigen Vorfällen, oder zur Berücksichtigung im Überprüfungsprozess für die Sicherheitspolitik dienen (siehe 3.2).

#### **6.3.5 Disziplinarverfahren**

Für Mitarbeiter, die Sicherheitspolitiken und -verfahren der Organisation verletzt haben, sollte ein formales Disziplinarverfahren vorhanden sein (siehe 6.1.4 und für die Aufbewahrung von Beweisen siehe 12.1.7). Ein derartiges Verfahren kann eine Abschreckung für Mitarbeiter darstellen, die sonst Sicherheitsverfahren missachten könnten. Zusätzlich sollte es eine korrekte, faire Behandlung von Mitarbeitern gewährleisten, die im Verdacht stehen, schwerwiegende oder wiederkehrende Sicherheitsverstöße zu begehen.

## **7 Physische und umgebungsbezogene Sicherheit**

### **7.1 Sicherheitszonen**

Ziel: Verhinderung von unberechtigtem Zugang, Beschädigung und Störung der Geschäftsräume und Informationen.

Verarbeitungsgeräte für wichtige oder sensitive Geschäftsinformationen sollten sich in Sicherheitszonen befinden, die durch eine definierte Sicherheitsgrenze geschützt und mit entsprechenden Sicherheitsschranken und Zutrittskontrollen versehen sind. Sie sollten physisch vor unberechtigtem Zugang, Beschädigung und Störung geschützt werden.

Der Schutz sollte den festgestellten Risiken angemessen sein. Es empfiehlt sich, eine Politik zum Aufräumen des Schreibtischs und Löschen des Bildschirms einzuführen, um das Risiko des unberechtigten Zugangs oder der Beschädigung von Papieren, Datenträgern und Geräten zur Informationsverarbeitung zu verringern.

#### **7.1.1 Physische Sicherheitsgrenze**

Physischer Schutz kann durch Errichtung mehrerer physischer Schranken um die Geschäftsräume und die Geräte zur Informationsverarbeitung herum erzielt werden. Jede Schranke bildet eine Sicherheitsgrenze,

die jede für sich den gesamten Schutz erhöht. Organisationen sollten Sicherheitsgrenzen einsetzen, um Bereiche zu schützen, die Geräte zur Informationsverarbeitung enthalten (siehe 7.1.3). Eine Sicherheitsgrenze ist etwas, das eine Schranke darstellt, z.B. eine Wand, eine kartengesteuerte Eintrittstür oder Mitarbeiter an der Rezeption. Die Lage und Stärke der einzelnen Schranken hängt von den Ergebnissen einer Risikoanalyse ab.

Folgende Richtlinien und Maßnahmen sollten bei Bedarf berücksichtigt und implementiert werden:

- a) Die Sicherheitsgrenze sollte klar definiert sein.
- b) Die Abgrenzung eines Gebäudes oder Standorts, das bzw. der Geräte zur Informationsverarbeitung enthält, sollte physisch intakt sein (d.h. es sollte keine Lücke in dieser Zone oder dieser Abgrenzung vorhanden sein, die ein müheloses Eindringen ermöglichen würde). Die Außenwände des Standorts sollten massiv gebaut und alle Außentüren durch geeignete Maßnahmen, z.B. Kontrollmechanismen, Riegel, Alarmgeräte, Schlösser usw., gegen unbefugten Zutritt geschützt sein.
- c) Es sollte ein Rezeptionsbereich mit Personal oder ein anderes Mittel vorhanden sein, um den physischen Zugang zum Standort oder zum Gebäude zu kontrollieren. Der Zutritt zu Standorten und Gebäuden sollte auf berechtigte Benutzer beschränkt werden.
- d) Zur Verhinderung von unberechtigtem Zutritt und Gefährdungen durch die Umwelt, wie Feuer und Überschwemmung, sollten physische Schranken, wenn nötig, vom Boden bis zur Decke ausgedehnt werden.
- e) Alle Feuerschutztüren einer Sicherheitsgrenze sollten mit einer Alarmanlage ausgestattet sein und selbsttätig schließen.

### **7.1.2 Physische Zutrittskontrollen**

Sicherheitszonen sollten durch entsprechende Zutrittskontrollen geschützt werden, um sicherzustellen, dass nur berechtigtem Personal Zutritt gestattet wird. Dabei sollten folgende Maßnahmen bedacht werden:

- a) Besucher von Sicherheitszonen sollten beaufsichtigt oder überprüft und Datum und Uhrzeit ihres Eintritts und Verlassens festgehalten werden. Ihnen sollte Zutritt nur für bestimmte, berechnete Zwecke gegeben werden. Außerdem sollten sie Anweisungen mit den Sicherheitsanforderungen des Bereichs und den Verfahrensweisen im Notfall erhalten.
- b) Der Zugang zu sensitiven Informationen und Geräten zur Informationsverarbeitung sollte kontrolliert und auf berechnete Personen beschränkt werden. Authentisierungskontrollen, wie Swipe-Cards plus PIN, sollten verwendet werden, um jeglichen Zugang zu autorisieren und zu bestätigen. Auditprotokolle über alle Zugangsversuche sollten an einem sicheren Ort aufbewahrt werden.
- c) Das gesamte Personal sollte sichtbare Kennungen tragen und unbegleitete Fremde und Personen ohne sichtbare Kennung zur Rede zu stellen.
- d) Zugangsrechte zu Sicherheitszonen sollten regelmäßig überprüft und auf den neuesten Stand gebracht werden.

### 7.1.3 Sicherung von Geschäftsräumen und Geräten

Bei einer Sicherheitszone kann es sich um ein abgeschlossenes Büro oder um mehrere Räume innerhalb einer physischen Sicherheitsgrenze handeln, die abgeschlossen werden können und abschließbare Schränke oder Tresore enthalten können. Die Wahl und die Anlage einer Sicherheitszone sollte die Möglichkeit eines Schadens durch Feuer, Überschwemmung, Explosionen, Unruhen und andere Formen der natürlichen oder durch Menschen verursachten Katastrophen berücksichtigen. Die Vorschriften und Normen zur Gesundheit und Sicherheit am Arbeitsplatz sollten ebenfalls beachtet werden. Sicherheitsbedrohungen, die durch angrenzende Räume bestehen, z.B. durch Wasserlecks in anderen Bereichen, sollten ebenfalls in Betracht gezogen werden.

Dabei sollte an folgende Maßnahmen gedacht werden:

- a) Der Standort für wichtige Geräte sollte so gewählt werden, dass kein öffentlicher Zugang besteht.
- b) Die Gebäude sollten nach Möglichkeit unauffällig sein und wenig Aufschluss über ihren Zweck geben. Keine augenfälligen Schilder außer- oder innerhalb des Gebäudes sollten auf die Existenz von Aktivitäten in der Informationsverarbeitung hinweisen.
- c) Support-Funktionen und -Geräte, z.B. Fotokopier-, Faxgeräte, sollten an geeigneter Stelle in der Sicherheitszone aufgestellt werden, um die Möglichkeit eines Zugangs zu unterbinden, der zur Kompromittierung von Informationen führen könnte.
- d) Türen und Fenster sollten verschlossen sein, wenn sie unbeaufsichtigt sind. Für Fenster, insbesondere solche im Erdgeschoss, sollte ein Außenschutz in Betracht gezogen werden.
- e) Geeignete Einbruchalarmsysteme sollten fachmännisch installiert und in regelmäßigen Abständen geprüft werden, um alle Außentüren und von außen zugängliche Fenster zu schützen. Leerstehende Bereiche sollten jederzeit durch einen Alarm gesichert sein. Schutzmaßnahmen sollten auch für andere Bereiche, z.B. Computerräume oder Räume mit Kommunikationseinrichtungen, vorgesehen werden.
- f) Geräte zur Informationsverarbeitung, die durch die Organisation verwaltet werden, sollten physisch von denen getrennt sein, die sich in der Verwaltung von Fremdunternehmen befinden.
- g) Verzeichnisse und interne Telefonbücher, die Standorte von sensitiven Geräten zur Informationsverarbeitung enthalten, sollten nicht öffentlich zugänglich sein.
- h) Gefährliche oder brennbare Materialien sollten entsprechend geschützt in sicherer Entfernung von der Sicherheitszone gelagert werden. Massengüter wie Papier sollten nicht vor ihrem Gebrauch in einer Sicherheitszone gelagert werden.
- i) Bereitschaftsgeräte und Backup-Datenträger sollten sich in sicherer Entfernung befinden, um vor den Folgen einer Katastrophe am Hauptstandort geschützt zu sein.

### 7.1.4 Arbeiten in Sicherheitszonen

Zusätzliche Maßnahmen und Richtlinien können zur Verbesserung der Sicherheit einer Sicherheitszone erforderlich sein. Hierzu zählen auch Maßnahmen für Mitarbeiter oder Fremdunternehmen, die in einer Sicherheitszone arbeiten, sowie für dort von Fremdunternehmen ausgeübte Aktivitäten. Folgende Punkte sollten berücksichtigt werden:

- a) Die Mitarbeiter sollten nur bei Bedarf über das Vorhandensein oder über Aktivitäten in einer Sicherheitszone informiert sein.
- b) Unbeaufsichtigte Tätigkeit in Sicherheitszonen sollte sowohl aus Sicherheitsgründen als auch zur Verhinderung von Gelegenheiten zu böswilligen Aktivitäten vermieden werden.
- c) Leerstehende Sicherheitszonen sollten physisch abgeschlossen und in regelmäßigen Zeitabständen überprüft werden.
- d) Support-Mitarbeiter von Fremdunternehmen sollten nur bei Bedarf eingeschränkten Zugang zu Sicherheitszonen oder sensitiven Geräten für die Informationsverarbeitung haben. Dieser Zugang sollte genehmigt und überwacht werden. Zusätzliche Schranken und Grenzen zur Kontrolle des physischen Zutritts können zwischen Bereichen mit unterschiedlichen Sicherheitsanforderungen innerhalb der Sicherheitszone vorgesehen werden.
- e) Fotoapparate, Video-, Audio- oder andere Aufzeichnungsgeräte sollten ohne ausdrückliche Genehmigung nicht zugelassen werden.

### 7.1.5 Separate Liefer- und Ladebereiche

Liefer- und Ladebereiche sollten kontrolliert und nach Möglichkeit von Geräten zur Informationsverarbeitung getrennt werden, um einen unberechtigten Zugang zu verhindern. Die Sicherheitsanforderungen für derartige Bereiche sollten durch eine Risikoanalyse bestimmt werden. Folgende Punkte sollten berücksichtigt werden:

- a) Der Zugang zum Lagerbereich von außen sollte sich auf identifiziertes und autorisiertes Personal beschränken.
- b) Der Lagerbereich sollte so angelegt sein, dass Zubehör abgeladen werden kann, ohne dass dem Lieferpersonal der Zutritt zu anderen Teilen des Gebäudes möglich ist.
- c) Die Außentür(en) des Lagerbereichs sollte(n) gesichert sein, wenn die Innentür geöffnet wird.
- d) Ankommendes Material sollte auf potentielle Gefahren (siehe 7.2. 1 d) **hin** untersucht werden, ehe es vom Lagerbereich an seinen Verwendungsort verlegt wird.
- e) Ankommendes Material sollte nach Möglichkeit (siehe 5. 1) bei Ankunft am Standort registriert werden.

## 7.2 Sicherheit der Geräte

Ziel: Verhinderung von Verlust, Beschädigung oder Kompromittierung von Werten und der Unterbrechung von Geschäftsaktivitäten.

Geräte sollten physisch vor Sicherheitsbedrohungen und umgebungsbedingten Gefahren geschützt werden.

Schutz von Geräten (einschließlich der auswärts benutzten) ist erforderlich, um das Risiko unberechtigten Zugangs zu Daten zu verringern und sich vor Verlust und Schaden zu schützen. Dies sollte auch bei der Aufstellung und Beseitigung der Geräte berücksichtigt werden. Besondere Maßnahmen müssen unter Umständen ergriffen werden, um sich vor Gefährdungen oder unberechtigtem Zugang zu schützen, und um unterstützende Einrichtungen wie die Stromversorgung und die Infrastruktur der Verkabelung zu sichern.

### 7.2.1 Positionierung und Schutz der Geräte

Die Positionierung und der Schutz von Geräten sollte so beschaffen sein, dass Risiken durch umgebungsbedingte Bedrohungen und Gefährdungen sowie Gelegenheiten für unberechtigten Zugang reduziert werden. Folgende Punkte sollten berücksichtigt werden:

- a) Geräte sollten so aufgestellt werden, dass unnötiger Zugang zu Arbeitsbereichen weitestgehend beschränkt wird.
- b) Geräte zur Informationsverarbeitung und -speicherung, mit denen sensitive Daten verarbeitet werden, sollten so aufgestellt werden, dass das Risiko der Einsichtnahme verringert wird.
- c) Gegenstände, die besonderen Schutz erfordern, sollten isoliert werden, um den Umfang der generell erforderlichen Schutzmaßnahmen zu verringern.
- d) Maßnahmen sollten angewendet werden, um das Risiko durch folgende Gefahrenquellen gering zu halten:
  - 1) Diebstahl
  - 2) Feuer
  - 3) Sprengstoffe
  - 4) Rauch
  - 5) Wasser (oder Ausfall der Wasserversorgung)
  - 6) Staub
  - 7) Schwingungen
  - 8) Chemische Einflüsse
  - 9) Störung der Stromversorgung
  - 10) Elektromagnetische Abstrahlung.
- e) Eine Organisation sollte ihre Politik hinsichtlich des Verzehrs von Speisen und Getränken und des Rauchens in der Nähe von Geräten zur Informationsverarbeitung überprüfen.

- f) Die Umgebung sollte daraufhin überprüft werden, ob sie sich nachteilig auf den Betrieb von Geräten zur Informationsverarbeitung auswirken könnte.
- g) Die Verwendung besonderer Schutzeinrichtungen wie Tastaturabdeckungen sollte für Geräte in industrieller Umgebung erwogen werden.
- h) Die Folgen einer Katastrophe, die sich in einem angrenzenden Bereich ereignet, z.B. Feuer in einem Nachbargebäude, Wassereintrich über das Dach oder in Untergeschosse oder eine Explosion auf der Straße, sollten geprüft werden.

### **7.2.2 Stromversorgung**

Geräte sollten vor Netzausfällen und anderen elektrischen Störungen geschützt werden. Es sollte eine geeignete Stromversorgung verfügbar sein, die den Spezifikationen des Geräteherstellers entspricht. Optionen zur Sicherung einer kontinuierlichen Stromversorgung sind:

- a) mehrere Versorgungsleitungen als vorbeugende Maßnahme gegen eine Stromunterbrechung beim Ausfall einer Leitung;
- b) unterbrechungsfreie Stromversorgung (USV);
- c) Notstromaggregat.

Für Geräte, die wichtige Geschäftsvorgänge unterstützen, wird eine unterbrechungsfreie Stromversorgung (USV) empfohlen, um ein ordnungsgemäßes Abschaltverfahren oder einen kontinuierlichen Betrieb zu gewährleisten. Notfallpläne sollten die Maßnahmen beschreiben, die bei Ausfall der USV ergriffen werden sollen. USV-Ausrüstung sollte in regelmäßigen Abständen auf angemessene Kapazität und gemäß den Empfehlungen des Herstellers getestet werden.

Wenn die Verarbeitung auch im Falle eines längeren Stromausfalls fortgesetzt werden soll, ist die Anschaffung eines Notstromaggregats zu erwägen. Nach der Installation sollten die Aggregate in regelmäßigen Abständen gemäß den Empfehlungen des Herstellers getestet werden. Es sollte eine ausreichende Menge an Kraftstoff vorhanden sein, um sicherzustellen, dass der Generator über einen verlängerten Zeitraum hinweg betrieben werden kann.

Darüber hinaus sollten sich Not-Ausschalter in der Nähe der Notausgänge der Betriebsräume befinden, um eine schnelle Stromabschaltung im Notfall zu ermöglichen. Bei Ausfall der gesamten Stromversorgung sollte eine Notbeleuchtung vorhanden sein. Alle Gebäude sollten mit einem Blitzschutz ausgestattet sein, und Blitzschutzfilter sollten bei allen externen Telekommunikationsleitungen installiert werden.

### **7.2.3 Sicherung der Verkabelung**

Strom- und Telekommunikationsverkabelung, die Daten überträgt oder Informationsdienste unterstützt, sollte vor Abhören oder Beschädigung geschützt werden. Dabei sollte an folgende Maßnahmen gedacht werden:

- a) Strom- und Telekommunikationskabel zu Geräten für die Informationsverarbeitung sollten nach Möglichkeit unterirdisch verlegt oder anderweitig angemessen geschützt werden.

- b) Netzverkabelung sollte z.B. durch Verwendung von Leitungsschutzrohren oder durch Vermeidung der Leitungsführung durch öffentliche Areale vor unberechtigtem Abhören oder Beschädigung geschützt werden.
- c) Stromkabel sollten von Telekommunikationskabeln getrennt werden, um eine gegenseitige Störung zu vermeiden.
- d) Bei sensitiven oder wichtigen Systemen sind weitere Maßnahmen wie folgt in Erwägung zu ziehen:
  - 1) Einbau von bewehrten Kabeln und verschlossenen Räumen oder Schließfächern an Inspektions- und Endpunkten;
  - 2) Verwendung alternativer Leitungsrührungen oder Übertragungsmedien;
  - 3) Verwendung von Glasfaserkabeln;
  - 4) Durchführung einer Aufspürprüfung für unberechtigte Geräte, die mit den Kabeln verbunden sind.

#### **7.2.4 Wartung der Geräte**

Geräte sollten ordnungsgemäß gewartet werden, um eine ununterbrochene Verfügbarkeit und Integrität zu gewährleisten. Folgende Punkte sollten berücksichtigt werden:

- a) Geräte sollten gemäß der vom Händler empfohlenen Service-Intervalle und Spezifikationen gewartet werden.
- b) Reparaturen und Service der Geräte sollten nur von berechtigtem Wartungspersonal durchgeführt werden.
- c) Es sollte eine Liste aller tatsächlichen oder vermuteten Fehler sowie aller vorbeugenden und fehlerbehebenden Wartungsarbeiten geführt werden.
- d) Beim Verschicken von Geräten zur Wartung außerhalb des Hauses sind entsprechende Maßnahmen zu ergreifen (siehe auch 7.2.6 hinsichtlich gelöschter und überschriebener Daten). Es sollten alle von den Versicherungspolicen auferlegten Anforderungen eingehalten werden.

#### **7.2.5 Sicherheit für Geräte außerhalb des Geschäftsgeländes**

Die Verwendung von allen Geräten für die Informationsverarbeitung außerhalb der Geschäftsräume ist unabhängig von der zuständigen Person durch das Management zu genehmigen. Die dabei bestehende Sicherheit sollte sich auf der gleichen Stufe befinden, wie bei den Geräten, die mit dem gleichen Zweck am Standort der Organisation verwendet werden, wobei die Risiken einer Tätigkeit außerhalb der Geschäftsräume der Organisation berücksichtigt wurden. Zur Ausstattung für die Informationsverarbeitung zählen alle Arten von PCs, Organismen, Mobiltelefonen, Papier oder andere Gegenstände, die für die Telearbeit genutzt oder vom normalen Arbeitsplatz entfernt werden. Folgende Punkte sollten berücksichtigt werden:

- a) Geräte und Datenträger, die aus den Geschäftsräumen mitgenommen wurden, sollten an öffentlichen Plätzen nicht unbeaufsichtigt gelassen werden. Tragbare Rechner sollten auf Reisen als Handgepäck und nach Möglichkeit verborgen getragen werden.

- b) Die Anleitungen des Herstellers zum Schutz der Geräte sollten jederzeit beachtet werden, um z.B. Schutz vor dem Aussetzen von starken elektromagnetischen Feldern zu bieten.
- c) Durch eine Risikoanalyse sollten geeignete Maßnahmen für die Telearbeit festgelegt werden. Es sind geeignete Maßnahmen, z.B. abschließbare Aktenschranke, Politik zur Aufräumspflicht und zu Zugangskontrollen für Computer, einzurühren.
- d) Es sollte ein entsprechender Versicherungsschutz bestehen, um die Geräte außerhalb der Geschäftsräume zu schützen.

Sicherheitsrisiken, **z.B.** durch Beschädigung, Diebstahl und Lauschangriffe, können von Ort zu Ort beachtlich variieren und sollten bei der Bestimmung der geeignetsten Maßnahmen berücksichtigt werden. Weitere Informationen zu den übrigen Punkten beim Schutz mobiler Geräte finden Sie unter 9.8.1.

### **7.2.6 Sichere Entsorgung oder Wiederverwendung von Geräten**

Informationen können durch unbedachte Entsorgung oder Wiederverwendung von Geräten (siehe auch 8.6.4) kompromittiert werden. Anstatt die herkömmliche Löschfunktion zu verwenden, sollten Speichergeräte mit sensitiven Informationen physisch vernichtet oder auf sichere Weise überschrieben werden.

Alle Geräte, die Speichermedien enthalten, z.B. Festplatten, sind zu überprüfen, um sicherzustellen, dass sensitive Daten und lizenzierte Software vor der Übergabe beseitigt oder überschrieben werden. Beschädigte Speichervorrichtungen, die sensitive Daten enthalten, können eine Risikoanalyse erforderlich machen, um zu bestimmen, ob die Teile vernichtet, repariert oder weggeworfen werden sollen.

### **7.3 Allgemeine Maßnahmen**

Ziel: Verhinderung der Kompromittierung oder des Diebstahls von Informationen und Geräten zur Informationsverarbeitung.

Informationen und Geräte zur Informationsverarbeitung sollten vor der Enthüllung, der Änderung oder dem Diebstahl durch unberechtigte Personen geschützt werden. Außerdem sollten Maßnahmen vorhanden sein, die den Verlust oder den Schaden verringern. Verfahren zur Behandlung und Speicherung werden in 8.6.3 erörtert.

#### **7.3.1 Politik zum Aufräumen des Schreibtischs und Löschen des Bildschirms**

Organisationen sollten die Einführung einer Politik zum Aufräumen von Papier und herausnehmbaren Speichermedien und eine Politik zum Löschen der Bildschirme von Geräten zur Informationsverarbeitung erwägen, um das Risiko des unberechtigten Zugriffs auf, des Verlusts von und des Schadens an Informationen während und außerhalb der normalen Arbeitszeit zu verringern. Diese Politik sollte die Einstufungen von Informationen (siehe 5.2), die entsprechenden Risiken und die kulturellen Aspekte der Organisation berücksichtigen.

Informationsträger, die auf Schreibtischen liegengelassen werden, können auch mit hoher Wahrscheinlichkeit bei einer Katastrophe wie einem Feuer, einer Überschwemmung oder einer Explosion vernichtet werden.

Daher sollten die folgenden Richtlinien eingehalten werden:

- a) Wenn notwendig, sollten Papiere und Computer-Disketten bei Nichtgebrauch und vor allem außerhalb der Arbeitszeiten in geeigneten abschließbaren Schränken und/oder anderen Arten von Sicherheitsmöbeln aufbewahrt werden.
- b) Sensitive und wichtige Geschäftsinformationen sollten, wenn sie nicht benötigt werden, vor allem beim Verlassen des Büros, weggeschlossen werden (am besten in einem feuerfesten Tresor oder Schrank).
- c) PCs, Rechnerterminals und Drucker sollten nicht angemeldet bleiben, wenn sie unbeaufsichtigt sind, und durch Schlösser, Passwörter oder durch andere Maßnahmen geschützt sein, wenn sie sich nicht in Gebrauch befinden.
- d) Orte für eingehende und ausgehende Post und unbeaufsichtigte Fax- und Telexgeräte sollten geschützt werden.
- e) Fotokopierer sollten außerhalb der Arbeitszeiten abgeschlossen sein oder auf andere Weise vor unberechtigter Benutzung geschützt werden.
- f) Sensitive oder eingestufte Informationen sollten sofort nach dem Ausdruck aus dem Drucker entfernt werden.

### **7.3.2 Entfernung von Eigentum**

Geräte, Informationen oder Software sollten nicht ohne Genehmigung des Managements aus dem Gebäude entfernt werden. Die Geräte sollten im Bedarfsfall (nach Notwendigkeit und Angemessenheit) abgemeldet und bei Rückkehr wieder angemeldet werden. Es sollten Stichproben durchgeführt werden, um eine unberechtigte Entfernung von Eigentum zu ermitteln. Die Mitarbeiter sollten daraufhingewiesen werden, dass Stichproben durchgeführt werden.

## **8 Management der Kommunikation und des Betriebs**

### **8.1 Betriebsverfahren und -Verantwortlichkeiten**

Ziel: Gewährleistung des korrekten und sicheren Betriebs von Geräten zur Informationsverarbeitung.

Verantwortlichkeiten und Verfahren für die Verwaltung und den Betrieb aller Geräte zur Informationsverarbeitung sollten eingeführt werden. Hierzu gehört auch die Erstellung von entsprechenden Betriebsanweisungen und Meldeverfahren für Vorfälle.

Eine Pflichtentrennung (siehe 8.1.4) sollte implementiert werden, um das Risiko des fahrlässigen oder absichtlichen Systemmissbrauchs zu reduzieren.

### 8.1.1 Dokumentierte Betriebsverfahren

Die durch die Sicherheitspolitik angegebenen Betriebsverfahren sollten dokumentiert und bei Bedarf überarbeitet werden. Die Betriebsverfahren sollten als formale Dokumente behandelt werden. Änderungen sind durch das Management zu genehmigen.

Die Verfahren sollten Anweisungen für die detaillierte Ausführung jeder Tätigkeit spezifizieren, und folgende Punkte beinhalten:

- a) Verarbeitung und Behandlung von Informationen.
- b) Anforderungsplanung, die die Abhängigkeit von anderen Systeme sowie den frühesten Zeitpunkt des Tätigkeitsbeginns und den spätesten Zeitpunkt des Tätigkeitsendes berücksichtigt.
- c) Anweisungen für die Fehlerbehandlung oder für den Umgang mit anderen Ausnahmebedingungen, die während der Ausführung einer Tätigkeit auftreten könnten, einschließlich Einschränkungen des Gebrauchs von Systemdienstprogrammen (siehe 9.5.5).
- d) Anlaufstellen für technische Unterstützung im Falle unerwarteter operativer oder technischer Schwierigkeiten.
- e) Spezielle Anweisungen für die Behandlung von Ausdrucken, wie die Verwendung speziellen Papiers oder das Management von vertraulichen Ausdrucken, einschließlich Verfahren für sichere Entsorgung von Fehldrucken.
- f) Neustart des Systems und bei einem Systemausfall anzuwendende Wiederherstellverfahren.

Dokumentierte Verfahren sollten auch für Systemverwaltungstätigkeiten im Zusammenhang mit Geräten zur Informationsverarbeitung und Kommunikation aufgestellt werden, wie für Rechnerinbetriebnahme und -abschaltverfahren, Datensicherung, Gerätewartung, Management und Sicherheit des Rechnerraums und der Behandlung von E-Mail.

### 8.1.2 Kontrolle von Veränderungen

Veränderungen bei Geräten und Systemen zur Informationsverarbeitung sollten überwacht werden. Unzureichende Kontrolle der Veränderungen bei Geräten und Systemen zur Informationsverarbeitung ist eine verbreitete Ursache von System- und Sicherheitsausfällen. Formale Verantwortlichkeiten und -verfahren sollten deshalb vorhanden sein, um eine zufriedenstellende Kontrolle aller Veränderungen bei Geräten, Software oder Verfahren zu gewährleisten. Betriebsprogramme sollten einer strengen Änderungskontrolle unterliegen. Bei der Änderung von Programmen sollte ein Auditprotokoll mit allen relevanten Informationen aufbewahrt werden. Änderungen in der Betriebsumgebung können sich auf die Anwendungen auswirken. Sofern es die Möglichkeiten zulassen, sollten die betrieblichen und anwendungsspezifischen Änderungskontrollverfahren integriert werden (siehe auch 10.5.1). Dabei sollten besonders die folgenden Punkte berücksichtigt werden:

- a) Feststellung und Aufzeichnung bedeutender Veränderungen;
- b) Beurteilung der potentiellen Auswirkung derartiger Veränderungen;

- c) Formales Genehmigungsverfahren für geplante Veränderungen.
- d) Mitteilung der Veränderungsdetails an alle betroffenen Personen;
- e) Verfahren zur Ermittlung von Verantwortlichkeiten für den Abbruch und die Wiederherstellung nach fehlgeschlagenen Veränderungen.

### 8.1.3 Verfahren für das Management von Vorfällen

Verantwortlichkeiten und Verfahren für das Management von Vorfällen sollten eingeführt werden, damit schnell, effektiv und ordnungsgemäß auf Sicherheitsvorfälle reagiert werden kann (siehe auch 6.3.1). Folgende Punkte sollten berücksichtigt werden:

- a) Es sollten Verfahren eingeführt werden, die alle möglichen Arten von Sicherheitsvorfällen erfassen. Dazu gehören:
  - 1) Ausfälle des Informationssystems und Verlust von Diensten.
  - 2) Verweigerung von Diensten (Denial of Service).
  - 3) Fehler aufgrund von unvollständigen oder ungenauen Geschäftsdaten.
  - 4) Vertraulichkeitsverstöße.
- b) Zusätzlich zu normalen Notfallplänen (für möglichst schnelle Wiederherstellung von Systemen oder Diensten) sollten in den Verfahren folgende Punkte enthalten sein (siehe auch 6.3.4):
  - 1) Analyse und Identifikation der Ursache des Vorfalls;
  - 2) sofern erforderlich, Planung und Implementierung von Gegenmaßnahmen zur Vermeidung eines erneuten Vorkommens;
  - 3) Sammeln von Auditprotokollen und ähnlichen Beweisen;
  - 4) Kommunikation mit denjenigen, die durch die Wiederherstellung nach dem Vorfall betroffen oder an ihr beteiligt sind;
  - 5) Meldung der Maßnahme an die entsprechenden Stellen.
- c) Auditprotokolle und ähnliche Beweise sollten nach Bedarf für folgende Zwecke gesammelt (siehe 12.1.7) und gesichert werden:
  - 1) interne Problemanalyse;
  - 2) Beweismittel im Zusammenhang mit potentiellm Vertragsbruch, Verstoß gegen Vorschriften oder bei zivil- oder strafrechtlichen Verfahren, z.B. bei Computermißbrauch oder Verstößen gegen die Datenschutzgesetzgebung;
  - 3) Verhandlungen mit Software- und Dienstbietern über Entschädigungsleistungen.
- d) Maßnahmen zur Wiederherstellung nach Sicherheitsverstößen und zur Behebung von Systemausfällen sollten sorgfältig und in einem formalen Verfahren kontrolliert werden. Die Verfahren sollten sicherstellen, dass:
  - 1) nur eindeutig identifizierte und berechnigte Mitarbeiter Zugang zu Systemen und Daten im aktiven Einsatz erhalten (siehe auch 4.2.2 für Zugang durch Fremdunternehmen);
  - 2) alle vorgenommenen Notfallmaßnahmen ausführlich dokumentiert werden;

- 3) Notfallmaßnahmen an das Management gemeldet und ordnungsgemäß nachgeprüft werden; die Integrität von Geschäftssystemen und Maßnahmen ohne Verzug bestätigt wird.

#### 8.1.4 Pflichtentrennung

Die Pflichtentrennung ist eine Methode zur Reduzierung des Risikos eines versehentlichen oder absichtlichen Systemmissbrauchs. Es sollte erwogen werden, das Management oder die Ausrührung bestimmter Pflichten oder Verantwortungsbereiche voneinander zu trennen, um Gelegenheiten für unberechtigte Änderungen oder den Missbrauch von Informationen oder Diensten zu reduzieren.

Für kleine Organisationen kann die Einführung dieser Maßnahme schwierig sein, aber das Prinzip sollte angewendet werden, soweit es möglich und praktikierbar ist. Wenn eine Trennung schwierig ist, sollten andere Maßnahmen wie z.B. eine Überwachung der Tätigkeiten, Auditprotokolle und eine Aufsicht durch das Management in Betracht gezogen werden. Es ist wichtig, dass das Sicherheitsaudit unabhängig bleibt.

Besonders sollte darauf geachtet werden, dass keine Person in Bereichen, für die sie allein verantwortlich ist, einen Betrug begehen kann, ohne dass dies bemerkt wird. Die Initiierung eines Vorfalls sollte von seiner Berechtigung getrennt werden. Folgende Punkte sollten berücksichtigt werden:

- a) Es ist wichtig, Tätigkeiten zu trennen, bei denen Absprachen für einen Betrug erforderlich sind, z.B. die Aufgabe einer Bestellung und die Überprüfung, ob die Waren eingegangen sind.
- b) Besteht die Gefahr von Absprachen, müssen Maßnahmen getroffen werden, um zwei oder mehr Personen an den Tätigkeiten zu beteiligen, damit auf diese Weise das Risiko möglicher Komplote gemindert wird.

#### 8.1.5 Trennung von Entwicklungs- und Betriebsanlagen

Eine Trennung der Entwicklungs-, Test- und Betriebsanlagen ist wichtig, um die daran beteiligten Rollen voneinander trennen zu können. Regeln für den Übergang von Software aus dem Entwicklungs- in den Betriebsstatus sollten definiert und dokumentiert werden.

Entwicklungs- und Testtätigkeiten können zu gravierenden Problemen führen, z.B. zu einer ungewollten Änderung von Dateien oder einer Systemumgebung oder zu einem Systemausfall. Das notwendige Ausmaß der Trennung zwischen Betriebs-, Test- und Entwicklungsumgebungen sollte in Betracht gezogen werden, um Betriebsprobleme zu verhindern. Eine ähnliche Trennung sollte auch zwischen den Entwicklungs- und Testfunktionen implementiert werden. In diesem Fall muss für eine bekannte und stabile Umgebung gesorgt werden, in der aussagekräftige Tests durchgeführt werden können und zu der es keinen ungeeigneten Zugang von Entwicklern gibt.

Sofern Entwicklungs- und Testmitarbeiter Zugriff auf das Betriebssystem und die darin enthaltenen Informationen haben, könnten sie unter Umständen unberechtigten und nicht getesteten Code einfügen oder Betriebsdaten ändern. Bei einigen Systemen könnte diese Zugriffsberechtigung zum Betrug missbraucht werden, oder nicht getesteter oder bösartiger Code eingerügt werden. Nicht getesteter oder bösartiger Code kann zu gravierenden Betriebsproblemen führen. Entwickler und Tester stellen auch eine Bedrohung für die Vertraulichkeit betrieblicher Informationen dar.

Entwicklungs- und Testtätigkeiten können unbeabsichtigte Änderungen an Software und Informationen herbeiführen, wenn sie dieselbe Rechnerumgebung teilen. Eine Trennung von Entwicklungs-, Test- und Betriebsgeräten ist deshalb wünschenswert, um das Risiko einer versehentlichen Änderung oder eines unberechtigten Zugriffs auf Betriebssoftware und Geschäftsdaten zu reduzieren. Dabei sollten folgende Maßnahmen in Betracht gezogen werden:

- a) Entwicklungs- und Betriebssoftware sollten nach Möglichkeit auf verschiedenen Computerprozessoren oder in unterschiedlichen Domänen oder Verzeichnissen laufen.
- b) Entwicklungs- und Testtätigkeiten sollten so weit wie möglich getrennt werden.
- c) Kompilierer, Editoren und andere Systemdienstprogramme sollten nicht von Betriebssystemen aufgerufen werden können, wenn dies nicht nötig ist.
- d) Für Betriebs- und Testsysteme sollten unterschiedliche Anmeldeverfahren verwendet werden, um das Fehlerrisiko einzuschränken. Benutzer sollten ermutigt werden, verschiedene Passwörter für diese Systeme zu verwenden, und Menüs sollten entsprechende Identifikationsmeldungen anzeigen.
- e) Entwicklungspersonal sollte nur dann Zugriff auf Passwörter für das Betriebssystem erhalten, wenn Maßnahmen vorhanden sind, um Passwörter für die Unterstützung von Betriebssystemen auszustellen. Mit Hilfe von Maßnahmen sollte sichergestellt werden, dass derartige Passwörter nach ihrer Benutzung geändert werden.

### **8.1.6 Externe Verwaltung von Geräten**

Die Verwendung eines externen Auftragnehmers für die Verwaltung von Geräten zur Informationsverarbeitung kann zu potentiellen Sicherheitsrisiken führen, wie z.B. einer Kompromittierung, einer Beschädigung oder einem Datenverlust am Standort des Auftragnehmers. Diese Risiken sollten vorab identifiziert und angemessene Maßnahmen mit dem Auftragnehmer vereinbart und in den Vertrag aufgenommen werden (siehe auch 4.2.2 und 4.3 zu Richtlinien für Verträge mit Fremdunternehmen, die einen Zugang zu Geräten der Organisation erhalten, und für Outsourcing-Verträge).

Besondere Punkte, die angesprochen werden sollten, sind:

- a) Identifizierung sensitiver oder kritischer Anwendungen, die möglichst in der Organisation bleiben sollten;
- b) Einholung von Genehmigungen der Personen, die für die Geschäftsanwendungen zuständig sind;
- c) Auswirkungen auf Pläne zur Aufrechterhaltung des Geschäftsbetriebs;
- d) zu spezifizierende Sicherheitsnormen und der Bewertungsprozess für deren Einhaltung;
- e) Zuweisung spezifischer Verantwortlichkeiten und Verfahren zur effektiven Kontrolle aller relevanten Sicherheitstätigkeiten;
- f) Verantwortlichkeiten und Verfahren für die Meldung und die Behandlung von Sicherheitsvorfällen (siehe 8.1.3).

## 8.2 Systemplanung und -abnahme

Ziel: Einschränkung des Risikos von Systemausfällen.

Vorausplanung und Vorbereitung sind erforderlich, um die Verfügbarkeit adäquater Kapazität und Ressourcen sicherzustellen.

Zur Einschränkung des Risikos einer Systemüberlastung sollten Vorausberechnungen von zukünftigen Kapazitätsanforderungen angestellt werden. Die Betriebsanforderungen neuer Systeme sollten vor ihrer Abnahme und Benutzung erstellt, dokumentiert und getestet werden.

### 8.2.1 Kapazitätsplanung

Kapazitätsanforderungen sollten überwacht und Vorausberechnungen zukünftiger Kapazitätsanforderungen angestellt werden, um sicherzustellen, dass eine ausreichende Verarbeitungsleistung und Speicherkapazität zur Verfügung stehen. Diese Vorausberechnungen sollten neue Geschäfts- und Systemanforderungen und aktuelle und vorhersehbare Trends der Informationsverarbeitung der Organisation berücksichtigen.

Großrechner erfordern besondere Aufmerksamkeit wegen der wesentlich höheren Kosten und längeren Beschaffungszeit für neue Kapazität. Manager von Großrechnerdiensten sollten den Gebrauch der wichtigsten Systemressourcen überwachen. Dazu gehören Prozessoren, Hauptspeicher, Datenspeicher, Drucker und andere Ausgabegeräte, sowie Kommunikationssysteme. Sie sollten Trends im Gebrauchs identifizieren, insbesondere in bezug auf Geschäftsanwendungen oder Tools für Managementinformationssysteme.

Manager sollten diese Informationen zur Identifizierung und Vermeidung potentieller Engpässe benutzen, die eine Bedrohung der Systemsicherheit oder der Benutzerdienste darstellen könnten, und entsprechende Abhilfe einplanen.

### 8.2.2 Systemabnahme

Abnahmekriterien für neue Informationssysteme, Updates und neue Versionen sollten geschaffen und geeignete Systemtests vor der Abnahme durchgeführt werden. Manager sollten sicherstellen, dass die Anforderungen und Kriterien für die Abnahme neuer Systeme klar definiert, vereinbart, dokumentiert und getestet werden. Folgende Punkte sollten in Betracht gezogen werden:

- a) Anforderungen an Leistungs- und Rechnerkapazität;
- b) Fehlerbehebungs- und Wiederanlaufverfahren sowie Notfallpläne;
- c) Vorbereitung und Tests von routinemäßigen Betriebsverfahren nach definierten Nonnen;
- d) vereinbarte und implementierte Maßnahmen;
- e) effektive manuelle Verfahren;
- f) Arrangements für die Aufrechterhaltung des Geschäftsbetriebs wie unter 11.1 gefordert;
- g) Nachweis, dass die Installation des neuen Systems existierende Systeme nicht beeinträchtigt, insbesondere zu Stoßzeiten der Verarbeitung wie dem Monatsende;

- h) Nachweis, dass die Auswirkung des neuen Systems auf die Gesamtsicherheit der Organisation bedacht worden ist;
- i) Schulungen für den Betrieb oder die Benutzung neuer Systeme.

Für wichtige neue Entwicklungen sollten während sämtlicher Stadien des Entwicklungsprozesses die Betriebsabteilung und die Benutzer befragt werden, um die betriebliche Leistungsfähigkeit der geplanten Systementwicklung sicherzustellen. Zur Bestätigung, dass alle Abnahmekriterien vollständig erfüllt werden, sollten entsprechende Tests durchgeführt werden.

### **8.3 Schutz vor bösartiger Software**

Ziel: Schutz der Integrität von Software und Informationen.

Vorsichtsmaßnahmen sind erforderlich, um die Einführung bösartiger Software zu verhindern und zu erkennen.

Software und Geräte zur Informationsverarbeitung sind durch die Einführung bösartiger Software wie z.B. Computerviren, Netzwürmer, trojanischer Pferde (siehe auch 10.5.4) und logischer Bomben gefährdet. Benutzer sollten über die Gefahren durch unberechtigte oder bösartige Software informiert werden und Manager sollten in entsprechenden Fällen spezielle Maßnahmen zur Erkennung oder Verhinderung der Einführung einer solchen Software treffen. Besonders wichtig ist, dass Vorsichtsmaßnahmen für die Erkennung oder Verhinderung von Computerviren bei PCs getroffen werden.

#### **8.3.1 Maßnahmen zum Schutz vor bösartiger Software**

Es sollten Erkennungs- und Verhinderungsmaßnahmen zum Schutz vor bösartiger Software sowie entsprechende Verfahren zur Schärfung des Benutzerbewusstseins implementiert werden. Der Schutz vor bösartiger Software sollte auf Sicherheitsbewusstsein, einem angemessenen Systemzugriff und Maßnahmen für das Management von Veränderungen beruhen. Folgende Maßnahmen sollten in Betracht gezogen werden:

- a) eine formale Sicherheitspolitik, bei der die Einhaltung der Softwarelizenzen verlangt und der Gebrauch unberechtigter Software untersagt wird (siehe 12.1.2.2);
- b) eine formale Sicherheitspolitik zum Schutz vor Risiken im Zusammenhang mit dem Erhalt von Dateien und Software von oder über externe Netze oder auf einem beliebigen anderen Datenträger mit Angabe darüber, welche Schutzmaßnahmen getroffen werden sollten (siehe auch 10.5, und insbesondere 10.5.4 und 10.5.5);
- c) Installation und regelmäßige Aktualisierung der Virenerkennungs- und Cleanerprogramme zum Durchsuchen nach Viren auf Rechnern und Datenträgern als Vorsichts- oder Routinemaßnahme;
- d) regelmäßige Überprüfungen der Software und des Dateninhalts von Systemen, die kritische Geschäftsprozesse unterstützen. Das Vorhandensein nicht genehmigter Dateien oder unerlaubter Änderungen sollte formal untersucht werden;
- e) Prüfung aller Dateien auf elektronischen Datenträgern, deren Herkunft ungewiß oder unzulässig ist, bzw. Dateien, die über nicht vertrauenswürdige Netze eingegangen sind, auf Viren vor dem Gebrauch;

- f) Prüfung aller E-Mail-Anhänge und Downloads auf bösartige Software vor dem Gebrauch; diese Prüfung kann an unterschiedlichen Stellen erfolgen, z.B. auf E-Mail-Servern, Desktop-Computern oder beim Eingang in das Netz der Organisation;
- g) Managementverfahren und -Verantwortlichkeiten in bezug auf den Virenschutz der Systeme, Schulungen zu deren Gebrauch und zur Meldung von und Wiederherstellung nach Virusangriffen (siehe 6.3 und 8.1.3);
- h) entsprechende Pläne zur Aufrechterhaltung des Geschäftsbetriebs nach
- i) Virusangriffen. Sie sollten alle erforderlichen Vorkehrungen für den Daten- und Software-back-up sowie für die Wiederherstellung beinhalten (siehe Abschnitt 11);
- j) Verfahren zur Verifikation sämtlicher Informationen in bezug auf bösartige Software und Sicherstellung, dass Warnmeldungen exakt und informativ sind. Manager sollten sicherstellen, dass kompetente Quellen, z.B. namhafte Zeitschriften, verlässliche Internet-Sites oder Hersteller von Antivirenprogrammen herangezogen werden, um zwischen Falschmeldungen über Viren und echten Viren zu unterscheiden. Mitarbeiter sollten auf das Problem von Falschmeldungen über Viren hingewiesen und informiert werden, was beim Empfang einer solchen Meldung zu tun ist.
- k) Diese Maßnahmen sind besonders für Netz-Dateiserver wichtig, die eine große Anzahl von Arbeitsstationen unterstützen.

## **8.4 Haushaltsorganisation**

Ziel: Aufrechterhaltung der Integrität und Verfügbarkeit von Diensten zur Informationsverarbeitung und zur Kommunikation.

Zur Durchführung der vereinbarten Back-up-Strategie (siehe 11.1) sollten Routineverfahren geschaffen werden, um Sicherungskopien von Datenbeständen zu erstellen und ihre schnelle Wiederherstellung zu üben. Vorfälle und Fehler zu protokollieren und, sofern angemessen, die Geräteumgebung zu überwachen.

### **8.4.1 Back-up von Informationen**

Sicherungskopien grundlegender Geschäftsinformationen und Software sollten regelmäßig erstellt werden. Adäquate Back-up-Einrichtungen sollten zur Verfügung stehen, damit wesentliche Geschäftsinformationen und Software nach einer Katastrophe oder nach einem Datenträgerausfall in ihrer Gesamtheit wiederhergestellt werden können.

Back-up- Arrangements für Einzelsysteme sollten regelmäßig getestet werden, um sicherzustellen, dass sie die Anforderungen der Pläne zur Aufrechterhaltung des Geschäftsbetriebs erfüllen (siehe Abschnitt 11). Folgende Richtlinien sollten in Betracht gezogen werden:

Ein Mindestmaß an Back-up-Informationen sollte zusammen mit exakten und vollständigen Aufzeichnungen über Sicherungskopien und dokumentierten Wiederherstellungsverfahren an einem entfernten Aufbewahrungsort gelagert werden. Dieser sollte sich in ausreichender Entfernung befinden, um einem Schaden durch eine Katastrophe am Hauptstandort zu entgehen. Für wichtige Geschäftsanwendungen sollten mindestens drei Generationen oder Zyklen von Back-up-Informationen aufbewahrt werden.

- a) Back-up-Informationen sollten ein geeignetes Maß an physischem und umgebungsbedingtem Schutz erhalten (siehe Abschnitt 7), das den anwendbaren Normen für Datenträger am Hauptstandort entspricht. Maßnahmen für Datenträger am Hauptstandort sollten erweitert werden, um den Back-up-Standort mit einzubeziehen.

- b) Sicherungsdenträger sollten, wenn praktikierbar, regelmäßig getestet werden, damit man sich im Notfall auf sie verlassen kann.
- c) Wiederherstellungsverfahren sollten regelmäßig geprüft und getestet werden, um sicherzustellen, dass sie effektiv sind und in dem Zeitrahmen, der in den Betriebsverfahren für die Wiederherstellung festgelegt ist, ausgeführt werden können.

Die Aufbewahrungsdauer für wesentliche Geschäftsinformationen sowie jeglicher Bedarf für eine ständige Aufbewahrung von Archivkopien (siehe 12.1.3) sollte festgelegt werden.

#### **8.4.2 Bedienerprotokolle**

Betriebsmitarbeiter sollten ihre Tätigkeiten protokollieren. Protokolle sollten je nach Angemessenheit die folgenden Punkte enthalten:

- a) Systemstart und -beendigungszeiten;
- b) Systemfehler und ausgeübte Korrekturtätigkeit;
- c) Bestätigung der korrekten Behandlung von Dateien und Rechnerausdrucken;
- d) den Namen der Person, die protokolliert.

Bedienerprotokolle sollten regelmäßigen, unabhängigen Prüfungen nach Betriebsabläufen unterworfen sein.

#### **8.4.3 Fehlerprotokoll**

Fehler sollten gemeldet und Korrekturmaßnahmen ergriffen werden. Von Benutzern gemeldete Fehler, die sich auf Probleme mit Systemen zur Informationsverarbeitung oder zur Kommunikation beziehen, sollten protokolliert werden. Es sollten klare Regeln für den Umgang mit gemeldeten Fehlern bestehen, z.B.:

- a) Überprüfung von Fehlerprotokollen zur Sicherstellung, dass Fehler zufriedenstellend behoben wurden;
- b) Überprüfung von Korrekturmaßnahmen, um sicherzustellen, dass Maßnahmen nicht kompromittiert wurden, und dass die ausgeführte Tätigkeit berechtigt war.

## 8.5 Netzwerkmanagement

Ziel: Sicherung von Informationen in Netzen und Schutz der unterstützenden Infrastruktur.

Das Sicherheitsmanagement von Netzen, die sich über die Grenzen der Organisation ausdehnen können, erfordert Aufmerksamkeit.

Zusätzliche Maßnahmen können ebenfalls erforderlich sein, um die Übermittlung sensibler Daten über öffentliche Netze zu schützen.

### 8.5.1 Netzwerk-Maßnahmen

Zum Erzielen und Bewahren von Sicherheit in Rechnernetzen sind eine Reihe von Maßnahmen erforderlich. Netzwerk-Manager sollten Maßnahmen implementieren, um die Datensicherheit in Netzen sowie den Schutz verbundener Dienste vor unberechtigtem Zugriff zu gewährleisten. Dabei sollten besonders die folgenden Punkte berücksichtigt werden:

- a) Wo notwendig, sollte die Verantwortlichkeit für den Netzbetrieb von derjenigen für den Rechnerbetrieb getrennt werden (siehe 8.1.4).
- b) Verantwortlichkeiten und Verfahren für das Management von entfernt gelegenen Anlagen, einschließlich Anlagen in Benutzerbereichen, sollten geschaffen werden.
- c) Wenn nötig, sollten besondere Maßnahmen getroffen werden, welche die Vertraulichkeit und Integrität von Daten, die über öffentliche Netze übertragen werden, sicherstellen und die vernetzten Systeme schützen (siehe 9.4 und 10.3). Besondere Maßnahmen können auch erforderlich sein, um die Verfügbarkeit der angeschlossenen Netzdienste und Rechner aufrechtzuerhalten.
- d) Managementtätigkeiten sollten eng koordiniert werden, um dem Unternehmen einen optimalen Service zu bieten und um sicherzustellen, dass die Maßnahmen konsistent über die gesamte informationsverarbeitende Infrastruktur angewendet werden.

## 8.6 Umgang mit und Sicherheit von Datenträgern

Ziel: Verhinderung von Schäden an Werten und Unterbrechungen des Geschäftsbetriebs. Datenträger sollten kontrolliert und physisch geschützt werden.

Geeignete Betriebsverfahren sollten geschaffen werden, um Dokumente, Datenträger (Bänder, Platten, Kassetten), Ein-/Ausgabedaten und Systemdokumentation vor Beschädigung, Diebstahl und unberechtigtem Zugriff zu schützen.

### 8.6.1 Verwaltung von mobilen Datenträgern

Es sollten Verfahren für die Verwaltung von mobilen Datenträgern, wie Bändern, Platten, Kassetten und gedruckte Aufzeichnungen, geschaffen werden. Folgende Richtlinien sollten in Betracht gezogen werden:

- a) Inhalte jedes wiederverwendbaren Datenträgers, der aus der Organisation entfernt werden soll, sollten gelöscht werden, wenn dafür kein Bedarf mehr besteht.

- b) Es sollte eine Genehmigungspflicht bestehen für alle Datenträger, die aus der Organisation entfernt werden, sowie eine Aufzeichnung all dieser beseitigten Datenträger, um ein Auditprotokoll aufrechtzuerhalten (siehe 8.7.2).
- c) Sämtliche Datenträger sollten in einer sicheren Umgebung gemäß den Spezifikationen des Herstellers aufbewahrt werden.

Alle Verfahren und Berechtigungsebenen sollten klar dokumentiert werden.

### **8.6.2 Beseitigung von Datenträgern**

Datenträger sollten sicher und zuverlässig beseitigt werden, wenn sie nicht mehr benötigt werden. Sensitive Informationen können durch eine nachlässige Beseitigung von Datenträgern an außenstehende Personen geraten. Es sollten formale Verfahren für die sichere Entsorgung von Datenträgern geschaffen werden, um dieses Risiko zu minimieren. Folgende Punkte sollten berücksichtigt werden:

- a) Datenträger, die sensitive Informationen enthalten, sollten sicher und zuverlässig aufbewahrt und entsorgt werden, z.B. durch Verbrennung oder durch den Reisswolf. Alternativ sollten die Daten gelöscht werden, um den Datenträger für den Gebrauch durch eine andere Anwendung innerhalb der Organisation zur Verfügung zu stellen.
- b) In der folgenden Liste sind Unterlagen aufgeführt, die gegebenenfalls sicher entsorgt werden müssen:
  - 1) Papierdokumente;
  - 2) Sprach- oder andere Aufzeichnungen;
  - 3) Kohlepapier;
  - 4) Ausgabedokumente;
  - 5) Einwegdruckerbänder;
  - 6) magnetische Bänder;
  - 7) auswechselbare Platten oder Kassetten;
  - 8) optische Speichermedien (alle Typen, einschließlich aller Software-Vertriebsmedien von Herstellern);
  - 9) Programmlisten;
  - 10) Testdaten;
  - 11) Systemdokumentation.
- c) Unter Umständen ist es einfacher, alle Datenträger zu sammeln und sicher beseitigen zu lassen, als zu versuchen, die sensitiven Elemente herauszusuchen.
- d) Viele Organisationen bieten Sammel- und Beseitigungsdienste für Papier, Geräte und Datenträger an. Bei der Auswahl eines geeigneten Auftragnehmers mit adäquaten Maßnahmen und ausreichender Erfahrung sollte sorgfältig vorgegangen werden.
- e) Die Beseitigung sensitiver Elemente sollte nach Möglichkeit zur lückenlosen Führung eines Auditprotokolls festgehalten werden.

Bei der Sammlung von zur Beseitigung anstehender Datenträger sollte dem Kumulationseffekt besondere Aufmerksamkeit zukommen. Dieser könnte bewirken, dass eine

große Menge nicht eingestufte Informationen sensibler ist als eine kleine Menge eingestufte Informationen.

### **8.6.3 Verfahren zum Umgang mit Informationen**

Es sollten Verfahren zur Behandlung und Speicherung von Informationen erstellt werden, um diese Informationen vor einer unberechtigten Offenlegung oder einem Missbrauch zu schützen. Es sollten Verfahren für die Behandlung von Informationen in Übereinstimmung mit ihrer jeweiligen Einstufung (siehe 5.2) entwickelt werden, für Informationen in Dokumenten, Computer-Systemen, Netzen, beim Mobile Computing, in der mobilen Kommunikation, bei E-mail und Post, bei Voice Mail, in der Sprachkommunikation allgemein, bei Multimedia-Anwendungen, bei Postdiensten/-einrichtungen, bei der Benutzung von Faxgeräten und anderen sensiblen Unterlagen, z.B. Blankoschecks, Rechnungen. Folgende Punkte sollten berücksichtigt werden (siehe auch 5.2 und 8.7.2):

- a) Behandlung und Kennzeichnung aller Datenträger (siehe auch 8.7.2a);
- b) Zugangsbeschränkungen zur Identifikation unberechtigten Personals;
- c) Führen einer formalen Aufzeichnung der berechtigten Datenempfänger;
- d) Sicherstellung, dass die Eingabedaten vollständig sind, dass der Verarbeitungsprozess ordnungsgemäß abgeschlossen wird, und dass die Ausgabedaten validiert werden;
- e) Schutz von Daten, die sich in einer Warteschlange befinden und mit dem Einstufungsgrad ausgegeben werden sollen, der der jeweiligen Sensitivität angemessen ist;
- f) Aufbewahrung von Datenträgern in einer Umgebung, die den Spezifikationen des Herstellers entspricht;
- g) Beschränkung der Verteilung von Daten auf ein Mindestmaß;
- h) deutliche Kennzeichnung aller Kopien von Daten für den berechtigten Empfänger;
- i) Überprüfung von Verteilerlisten und Listen berechtigter Empfänger in regelmäßigen Abständen.

### **8.6.4 Sicherheit von Systemdokumentation**

Systemdokumentation kann eine Reihe sensibler Informationen, z.B. Beschreibungen von Anwendungsprozessen, Verfahren, Datenstrukturen, Berechtigungsprozessen enthalten (siehe auch 9.1). Die folgenden Maßnahmen sollten in Betracht gezogen werden, um Systemdokumentation vor einem unberechtigten Zugang zu schützen:

- a) Systemdokumentation sollte sicher aufbewahrt werden.
- b) Die Zugangsliste auf Systemdokumentation sollte möglichst klein gehalten und von der für die Anwendung zuständigen Person genehmigt werden.
- c) Systemdokumentation, die auf einem öffentlichen Netz aufbewahrt wird oder über ein öffentliches Netz empfangen wird, sollte angemessen geschützt werden.

## 8.7 Austausch von Informationen und Software

Ziel: Verhinderung von Verlust, Änderung oder Missbrauch von Informationen, die zwischen Organisationen ausgetauscht werden.

Der Austausch von Informationen und Software zwischen Organisationen sollte kontrolliert werden und mit der jeweils anwendbaren Gesetzgebung übereinstimmen (siehe Abschnitt 12).

Ein Austausch sollte auf der Basis von Vereinbarungen unternommen werden. Es sollten Verfahren und Normen zum Schutz der Informationen und Datenträger im Transit geschaffen werden. Berücksichtigt werden sollten die Auswirkungen auf das Geschäft und die Sicherheit, die in Verbindung mit einem elektronischen Datenaustausch, E-Commerce und E-Mail entstehen könnten, sowie die Forderung nach Maßnahmen.

### 8.7.1 Vereinbarungen für den Austausch von Informationen und Software

Vereinbarungen, die in einigen Fällen formal sein können und in entsprechenden Fällen Software-Treuhandverträge einschließen, sollten für den (elektronischen oder manuellen) Austausch von Informationen und Software zwischen Organisationen getroffen werden. Der Sicherheitsinhalt einer derartigen Vereinbarung sollte die Sensitivität der betreffenden Geschäftsinformationen widerspiegeln. Vereinbarungen über Sicherheitsbedingungen sollten folgendes berücksichtigen:

- a) Verantwortung des Managements für die Kontrolle und Benachrichtigung von Übertragungen, Versand und Empfang;
- b) Meldeverfahren für Absender, Übertragung, Versand und Empfang;
- c) Mindestmaß an technischen Normen für Verpackung und Übertragung;
- d) Normen zur Identifikation von Boten;
- e) Verantwortlichkeiten und Haftung im Falle eines Datenverlusts;
- f) Benutzung eines vereinbarten Kennzeichnungssystems für sensitive oder kritische Informationen, um sicherzustellen, dass die Beschriftungen sofort verstanden werden, und dass die Informationen angemessen geschützt werden;
- g) Eigentum von Informationen und Software und Verantwortlichkeiten für Datenschutz, Einhaltung des Software-Urheberrechts und ähnliche Überlegungen (siehe 12.1.2 und 12.1.4);
- h) technische Normen zur Aufzeichnung und zum Lesen von Informationen und Software;
- i) spezielle Maßnahmen, die erforderlich sein können, um sensitive Elemente zu schützen, z.B. kryptographische Schlüssel (siehe 10.3.5).

### 8.7.2 Sicherheit von Datenträgern im Transit

Informationen können schutzlos gegen einen unberechtigten Zugriff, Missbrauch oder Beschädigung während eines physischen Transports sein, z.B. beim Übersenden von Datenträgern per Post oder Boten. Zur Sicherung des Transports von Datenträgern zwischen verschiedenen Standorten sollten die folgenden Maßnahmen getroffen werden:

- a) Es sollten zuverlässige Transportmittel oder Botendienste eingesetzt werden. Eine Liste berechtigter Boten sollte mit dem Management vereinbart werden, und ein Verfahren zur Identifikation von Boten sollte implementiert werden.
- b) Die Verpackung sollte ausreichend sein und den Spezifikationen des Herstellers entsprechen, um den Inhalt vor physischem Schaden zu schützen, der während des Transits entstehen kann.
- c) Spezielle Maßnahmen sollten in entsprechenden Fällen angewendet werden, um sensitive Informationen vor unberechtigter Veröffentlichung oder Änderung zu schützen. Beispiele sind:
  - 1) Verwendung verschlossener Behälter;
  - 2) persönliche Zustellung;
  - 3) beschädigungsresistente Verpackung (die jeden Versuch eines Zugangs anzeigt);
  - 4) In außergewöhnlichen Fällen Verteilung der Sendung auf mehr als eine Lieferung und Versand über verschiedene Wege.

### 8.7.3 E-Commerce-Sicherheit

Beim E-Commerce können elektronischer Datenaustausch (EDI), E-Mail und Online-Transaktionen über öffentliche Netze wie z.B. das Internet eingesetzt werden. E-Commerce ist einer Vielzahl von Netzwerkbedrohungen ausgesetzt, die zu betrügerischer Tätigkeit, vertragliche Streitigkeiten und die Offenlegung und Änderung von Informationen rühren können. Maßnahmen sollten getroffen werden, um E-Commerce vor diesen Bedrohungen zu schützen. Bei Sicherheitsüberlegungen für E-Commerce sollten folgende Punkte in Betracht gezogen werden:

- a) Authentisierung.  
Wieviel Vertrauen in die vom anderen vorgegebene Identität ist für Kunde und Händler notwendig?
- b) Berechtigung.  
Wer ist berechtigt, Preise festzusetzen, wichtige Handelsdokumente auszustellen oder zu unterschreiben? Wie weiß der Handelspartner das?
- c) Vertrags- und Ausschreibungsprozesse.  
Was sind die Forderungen in puncto Vertraulichkeit, Integrität und Beleg des Versands und Empfangs wichtiger Dokumente und hinsichtlich der Nicht-Abstreitbarkeit von Verträgen?
- d) Preisinformationen.  
Wieviel Vertrauen kann in die Integrität der ausgeschriebenen Preisliste und die Vertraulichkeit sensibler Rabattabsprachen gesetzt werden?
- e) Auftragstransaktionen.  
Wie wird für die Vertraulichkeit und Integrität der Auftrags-, Zahlungs- und Lieferadressenangaben und die Empfangsbestätigung gesorgt?
- f) Überprüfung.  
Wie hoch sollte der Grad der Überprüfung sein, um Zahlungsinformationen zu überprüfen, die vom Kunden angegeben wurden?
- g) Begleichung.  
Welches ist die geeignetste Zahlungsform zum Schutz vor Betrug?
- h) Bestellung.  
Was für ein Schutz ist erforderlich, um die Vertraulichkeit und Integrität der Bestellinformationen zu bewahren, und um den Verlust oder die Duplizierung von Transaktionen zu verhindern?
- i) Haftung.  
Wer trägt das Risiko für betrügerische Transaktionen?

Vielen der obigen Betrachtungen kann durch die Anwendung von kryptographischen Verfahren begegnet werden, die unter 10.3 erläutert sind, wobei berücksichtigt werden muss, dass diese im Einklang mit der jeweiligen Gesetzgebung stehen (siehe 12.1, insbesondere 12.1.6 zur Gesetzgebung zum Einsatz von kryptographischen Verfahren).

E-Commerce-Abkommen zwischen Handelspartnern sollten durch eine dokumentierte Vereinbarung unterstützt werden, die beide Parteien an die vereinbarten Handelsbedingungen, einschließlich der Berechtigungsdetails [siehe b) oben] bindet. Andere Vereinbarungen mit Informationsdienst- und Netzwerkanbietern mit zusätzlichen Leistungen sind unter Umständen notwendig.

Öffentliche Handelssysteme sollten ihren Kunden ihre Geschäftsbedingungen mitteilen. Bedacht werden sollten die Widerstandsfähigkeit gegen Angriffe auf den Host, der für den E-Commerce benutzt wird, und die Auswirkungen auf die Sicherheit der Netzverbindungen, die für diese Implementierung erforderlich sind (siehe 9.4.7).

## **8.7.4 E-Mail-Sicherheit**

### **8.7.4.1 Sicherheitsrisiken**

E-Mail wird immer häufiger für Geschäftskommunikation benutzt und ersetzt damit traditionelle Kommunikationsformen wie Telexe und Briefe. E-Mail unterscheidet sich von traditionellen Formen der Geschäftskommunikation beispielsweise durch Geschwindigkeit, Struktur der Nachricht, informellen Charakter und ihre Schutzlosigkeit gegenüber unberechtigten Aktivitäten. Bedacht werden sollte der Bedarf an Maßnahmen zur Reduzierung der Sicherheitsrisiken, die durch E-Mail entstehen. Sicherheitsrisiken sind z.B.:

- a) Schutzlosigkeit von Nachrichten gegen unberechtigte Zugriffe oder Änderungen oder Abstreitung einer Dienstleistung;
- b) Anfälligkeit für Fehler, z.B. falsche Adressierung oder Fehlleitung und die allgemeine Zuverlässigkeit und Verfügbarkeit des Dienstes;
- c) Auswirkung der Veränderung des Kommunikationsmediums auf Geschäftsprozesse, z.B. die Auswirkung von erhöhter Geschwindigkeit des Versands oder die Auswirkung des Versands förmlicher Mitteilungen von einer Person zur anderen und nicht von einem Unternehmen zum anderen;
- d) Gesetzliche Überlegungen, wie z.B. der potentielle Bedarf an Beweisen für Herkunft, Versand, Lieferung und Annahme;
- e) Auswirkungen durch die Veröffentlichung extern zugänglicher Mitarbeiterlisten;
- f) Kontrolle des Fernzugriffs von Benutzern auf E-Mail-Accounts.

### **8.7.4.2 E-Mail-Politik**

Organisationen sollten eine klare Politik in bezug auf die Verwendung von E-Mail aufstellen, die auch die folgenden Punkte berücksichtigt:

- a) Angriffe auf E-Mail, z.B. Viren, Abfangen von E-Mails;
- b) Schutz von E-Mail-Anhängen;
- c) Richtlinien, wann E-Mail nicht benutzt werden soll;

- d) Verantwortlichkeit des Mitarbeiters, das Unternehmen nicht zu kompromittieren, z.B. durch Senden verleumderischer E-Mails, die Benutzung zur Belästigung anderer, unberechtigte Käufe;
- e) Benutzung von kryptographischen Verfahren zum Schutz der Vertraulichkeit und Integrität von E-Mails (siehe 10.3);
- f) Aufbewahrung von Nachrichten, die, wenn sie gespeichert sind, im Falle eines Rechtsstreits entdeckt werden könnten;
- g) zusätzliche Maßnahmen zur Überprüfung von Nachrichten, die nicht authentisiert werden können.

### 8.7.5 Sicherheit elektronischer Bürosysteme

Politiken und Richtlinien sollten für die Kontrolle der Geschäfts- und Sicherheitsrisiken im Zusammenhang mit elektronischen Bürosystemen vorbereitet und implementiert werden. Diese Systeme bieten Möglichkeiten für eine schnellere Verteilung und gemeinsame Nutzung von Geschäftsinformationen durch eine Kombination aus: Dokumenten, Computern, Mobile Computing, mobilen Kommunikationen, E-Mail, Voice Mail, Sprachkommunikation allgemein, Multimedia-Anwendungen, Postdienstleistungen und Faxgeräten.

Bei der Betrachtung der Auswirkungen auf die Sicherheit und das Geschäft bei einer Verbindung dieser Einrichtungen sollten folgende Punkte berücksichtigt werden:

- a) Schutzlosigkeit von Informationen in Bürosystemen, z.B. Aufzeichnung von Telefonaten oder Konferenzschaltungen, Vertraulichkeit von Telefonaten, Speicherung von Faxen, Öffnen von Post, Verteilen von Post;
- b) Politik und entsprechende Maßnahmen zur Verwaltung gemeinsamer Informationen, z.B. die Verwendung unternehmenseigener elektronischer Anschlagtafeln (siehe 9.1);
- c) Ausschluss von Kategorien sensibler Geschäftsinformationen, wenn das System keinen angemessenen Schutz bietet (siehe 5.2);
- d) Beschränkung des Zugriffs auf Informationen in Terminplanen, die bestimmte Einzelpersonen betreffen, z.B. Mitarbeiter, die an sensiblen Projekten arbeiten;
- e) Eignung oder Nichteignung des Systems für die Unterstützung von Geschäftsanwendungen, wie zur Mitteilung von Befehlen oder Genehmigungen;
- f) Kategorien von Mitarbeitern, Auftragnehmern oder Geschäftspartnern, die das System und die Standorte, von denen der Zugang möglich ist, benutzen dürfen (siehe 4.2);
- g) Beschränkung ausgewählter Einrichtungen auf spezifische Benutzerkategorien;
- h) Identifizierung des Status von Benutzern, z.B. Mitarbeiter der Organisation oder Auftragnehmer in Verzeichnissen, für den Gebrauch anderer Benutzer;
- i) Aufbewahrung und Back-ups von im System befindlichen Informationen (siehe 12.1.3 und 8.4.1);
- j) Reserveanforderungen und -Arrangements (siehe 11.1).

### 8.7.6 Öffentlich zugängliche Systeme

Die Integrität elektronisch publizierter Informationen sollte sorgfältig geschützt werden, um unberechtigte Änderungen zu verhindern, die den Ruf der veröffentlichenden Organisation

schädigen könnten. Informationen auf einem öffentlich zugänglichen System, z.B. Informationen auf einem Web-Server, auf die über das Internet zugegriffen werden kann, müssen unter Umständen mit Gesetzen, Regeln und Vorschriften der jeweils anwendbaren Gesetzgebung im Einklang stehen, in der das System steht oder wo der Handel stattfindet. Es sollte ein formaler Genehmigungsprozess bestehen, bevor Informationen öffentlich bereitgestellt werden.

Software, Daten und andere Informationen, für die ein hoher Grad an Integrität erforderlich ist und die auf einem öffentlich zugänglichen System bereitgestellt werden, sollten durch entsprechende Mechanismen geschützt werden, z.B. digitale Signaturen (siehe 10.3.3). Elektronische Veröffentlichungssysteme, insbesondere solche, die Feedbacks und eine direkte Eingabe von Informationen erlauben, sollten sorgfältig kontrolliert werden, damit

- a) Informationen im Einklang mit der jeweiligen Datenschutzgesetzgebung erhalten werden (siehe 12.1.4);
- b) Informationen, die in das Veröffentlichungssystem eingegeben und dort verarbeitet werden, vollständig, korrekt und zügig verarbeitet werden;
- c) sensitive Informationen während des Sammelprozesses und bei der Aufbewahrung geschützt werden;
- d) ein Zugriff auf das Veröffentlichungssystem keinen unbeabsichtigten Zugriff auf Netze erlaubt, mit denen es verbunden ist.

### **8.7.7 Andere Formen des Informationsaustausches**

Es sollten Verfahren und Maßnahmen vorhanden sein, um den Austausch von Informationen über Sprach-, Fax- und Videokommunikationsgeräte zu schützen. Informationen könnten aufgrund eines mangelnden Bewusstseins, mangelnder Politik oder mangelnder Verfahren zur Benutzung derartiger Geräte kompromittiert werden, z.B. durch Mithörer bei einem Gespräch über ein Handy an einem öffentlichen Platz, Mithörer von Nachrichten auf Anrufbeantwortern, unerlaubten Zugriff auf Voice Mail-Systeme, in die man sich einwählen kann, oder durch das versehentliche Senden von Faxen über das Faxgerät an die falsche Person.

Geschäftsabläufe könnten gestört und Informationen kompromittiert werden, wenn Kommunikationsgeräte versagen, überlastet sind oder unterbrochen werden (siehe 7.2 und Abschnitt 11). Informationen könnten auch kompromittiert werden, wenn unberechtigte Benutzer auf sie zugreifen (siehe Abschnitt 9).

Eine klare Erklärung der Politik mit Verfahren, die Mitarbeiter bei der Benutzung von Sprach-, Fax- und Videokommunikationsgeräten befolgen müssen, sollte aufgestellt werden.

Diese sollte folgende Punkte enthalten:

- a) Erinnerung der Mitarbeiter, dass sie entsprechende Vorsichtsmaßnahmen treffen sollten, z.B. keine sensitiven Informationen aussprechen sollten, wenn die Gefahr besteht, dass ihr Telefonat mit- oder abgehört wird:
  - 1) von Personen in ihrer direkten Umgebung, insbesondere beim Telefonieren mit einem Handy;
  - 2) durch angezapfte Leitungen und andere Formen des Belauschens durch physischen Zugang zum Handapparat oder zur Telefonleitung oder durch die Verwendung von Suchempfängern bei Benutzung analoger Handys;

- 3) durch Personen auf der Seite des Gesprächspartners;
- b) Erinnerung der Mitarbeiter, dass sie keine vertraulichen Gespräche an öffentlichen Plätzen oder Großraumbüros und an Treffpunkten mit dünnen Wänden führen sollten;
- c) Es sollten keine Nachrichten auf Anrufbeantwortern hinterlassen werden, da diese von unberechtigten Personen abgespielt, auf gemeinschaftlichen Systemen oder aufgrund von Verwählen falsch abgespeichert werden könnten;
- d) Erinnerung der Mitarbeiter an Probleme in Verbindung mit der Benutzung von Faxgeräten, nämlich:
  - 1) unberechtigter Zugriff auf eingebaute Nachrichtenspeicher zum Abrufen von Mitteilungen;
  - 2) absichtliche oder versehentliche Programmierung von Geräten, um Mitteilungen an bestimmte Nummern zu senden;
  - 3) Senden von Dokumenten und Mitteilungen an die falsche Nummer, entweder durch Verwählen oder durch Benutzung der falschen Nummer im Speicher.

## **9 Zugangskontrolle**

### **9.1 Geschäftsanforderungen an die Zugangskontrolle**

Ziel: Kontrolle des Zugangs zu Informationen.

Der Zugang zu Informationen und Geschäftsprozessen sollte auf der Basis von Geschäfts- und Sicherheitsanforderungen kontrolliert werden.

Dabei sollten Politiken für die Informationsverbreitung und Zugriffsberechtigung berücksichtigt werden.

#### **9.1.1 Zugangskontrollpolitik**

##### **9.1.1.1 Politik und Geschäftsanforderungen**

Geschäftsanforderungen an die Zugangskontrolle sollten definiert und dokumentiert werden. Regeln und Rechte der Zugangskontrolle für jeden Benutzer oder jede Gruppe von Benutzern sollten in einer Erklärung der Zugangspolitik unmissverständlich aufgeführt werden. Benutzer und Diensteanbieter sollten eine klare Aufstellung der Geschäftsanforderungen erhalten, die von Zugangskontrollen erfüllt werden müssen.

Die Politik sollte die folgenden Punkte berücksichtigen:

- a) Sicherheitsanforderungen einzelner Geschäftsanwendungen;
- b) Identifikation sämtlicher Informationen im Zusammenhang mit den Geschäftsanwendungen;
- c) Politiken für die Informationsverbreitung und Zugriffsberechtigung, z.B. das Prinzip „Kenntnis nur wenn nötig“, sowie Sicherheitsniveaus und die Einstufung von Informationen;

- d) Konsistenz zwischen den Politiken zur Zugangskontrolle und den Informationseinstufung verschiedener Systeme und Netze;
- e) relevante Gesetzgebung und jegliche vertragliche Verpflichtungen in bezug auf den Zugangsschutz für Daten oder Dienste (siehe Abschnitt 12);
- f) Profile des standardmäßigen Benutzerzugriffs für übliche Jobkategorien;
- g) Verwaltung von Zugriffsrechten in einer verteilten und vernetzten Umgebung, die alle zur Verfügung stehenden Verbindungen erkennt.

### 9.1.1.2 Regeln für die Zugangskontrolle

Bei der Spezifizierung der Regeln für die Zugangskontrolle sollten die folgenden Punkte sorgfältig bedacht werden:

- a) Unterscheidung zwischen Regeln, die zwingend vorgeschrieben sind und Regeln, die optional oder vorbehaltlich sind;
- b) Aufstellung von Regeln, die auf der Prämisse „Alles was nicht ausdrücklich erlaubt ist, ist verboten“ basieren und nicht auf der schwächeren Regel „Generell ist alles erlaubt, außer es ist ausdrücklich verboten“;
- c) Änderungen bei Kennzeichnungen von Informationen (siehe 5.2), die automatisch von Geräten zur Informationsverarbeitung eingeführt werden, und solche, die nach eigenem Ermessen eines Benutzers eingeführt werden;
- d) Änderungen von Benutzerberechtigungen, die automatisch vom Informationssystem eingeführt werden und solche, die von einem Administrator eingeführt werden;
- e) Regeln, für die vor der Ausführung eine Genehmigung seitens des Administrators oder einer anderen Person eingeholt werden muss, und Regeln, bei denen dies nicht erforderlich ist.

## 9.2 Verwaltung der Zugriffsrechte der Benutzer

Ziel: Verhinderung des unberechtigten Zugriffs auf Informationssysteme.

Zur Kontrolle der Zuteilung von Zugriffsrechten auf Informationssysteme und -dienste sollten formale Verfahren bestehen.

Diese Verfahren sollten sich auf sämtliche Stadien im Lebenszyklus des Benutzerzugriffs beziehen, von der erstmaligen Anmeldung neuer Benutzer bis zur endgültigen Abmeldung von Benutzern, die keinen Zugriff auf Informationssysteme und -dienste mehr benötigen. In entsprechenden Fällen sollte besonders die Notwendigkeit beachtet werden, die Zuteilung privilegierter Zugriffsrechte zu kontrollieren, durch die es Benutzern erlaubt wird, Systemkontrollen zu übergehen.

### 9.2.1 Anmeldung von Benutzern

Es sollte ein formales Anmelde- und Abmeldeverfahren für Benutzer existieren, die den Zugriff auf alle Multi-User-Informationssysteme und -dienste regeln.

Der Zugriff auf Multi-User-Informationsdienste sollte durch einen formalen Anmeldeprozess für Benutzer kontrolliert werden, der folgendes beinhalten sollte:

- a) Verwendung eindeutiger Benutzerkennungen, so dass alle Tätigkeiten zu ihren Benutzern zurückverfolgt und diese dafür verantwortlich gemacht werden können. Die Verwendung von Gruppenkennungen sollte nur erlaubt werden, wenn sie sich für die ausgerichtete Arbeit eignen;
- b) Prüfung, ob der Benutzer von der für das System zuständigen Person eine Berechtigung zur Benutzung des Informationssystems oder -dienstes hat. Eine getrennte Genehmigung des Managements für Zugriffsrechte könnte ebenfalls angebracht sein;
- c) Prüfung, ob der genehmigte Grad des Zugriffs mit den Geschäftszwecken vereinbar (siehe 9.1) und konsistent mit der Sicherheitspolitik der Organisation ist, z.B. ob die Pflichtentrennung nicht kompromittiert wird (siehe 8.1.4);
- d) Übergabe einer schriftlichen Aufstellung ihrer Zugriffsrechte an die Benutzer;
- e) Unterschrift der Benutzer von Erklärungen, dass sie die Zugriffsbedingungen verstehen;
- f) Sicherstellung, dass Diensteanbietern kein Zugriff gewährt wird, bevor das Berechtigungsverfahren abgeschlossen wurde;
- g) Führen einer formalen Aufzeichnung aller Personen, die für die Benutzung des Dienstes angemeldet sind;
- h) sofortige Aufhebung der Zugriffsrechte für Benutzer, die die Stelle gewechselt oder die Organisation verlassen haben;
- i) regelmäßige Prüfung und Löschung redundanter Benutzerkennungen und -accounts;
- j) Sicherstellung, dass keine redundanten Benutzerkennungen an andere Benutzer ausgestellt werden.

In Betracht gezogen werden sollte auch eine Aufnahme von Klauseln in Mitarbeiter- und Dienstleistungsverträgen, in denen Strafmaßnahmen für einen unberechtigten Zugriffsversuch durch eigene Mitarbeiter oder die Mitarbeiter der Diensteanbieter festgelegt werden (siehe auch 6.1.4 und 6.3.5).

### **9.2.2 Verwaltung von Privilegien**

Die Zuteilung und Nutzung von Privilegien (jede Funktion oder Einrichtung in einem Multi-User-Informationssystem, die es dem Benutzer erlaubt, System- oder Anwendungskontrollen zu übergehen) sollten beschränkt und kontrolliert werden. Eine unangemessene Nutzung von Systemprivilegien ist oft ein wichtiger Faktor für das Versagen von Systemen, in die eingedrungen wurde.

Bei Multi-User-Systemen, die vor unberechtigten Zugriffen geschützt werden müssen, sollte die Zuteilung von Privilegien durch einen formalen Berechtigungsprozess kontrolliert werden. Folgende Schritte sollten in Betracht gezogen werden:

- a) Die Privilegien in Verbindung mit jedem Systemprodukt, z.B. Betriebssystem, Datenbankverwaltungssystem und jeder Anwendung, sowie die Mitarbeiterkategorien, denen sie zugesprochen werden sollen, sollten identifiziert werden.

- b) Privilegien sollten Einzelpersonen auf einer Basis, die sich nach dem Anwendungsbedarf und dem jeweiligen Fall richtet, zugesprochen werden, d.h. den minimalen Anforderungen für ihre Funktion in der Organisation entsprechend und nur bei Bedarf.
- c) Ein Berechtigungsprozess und eine Aufzeichnung aller erteilten Privilegien sollten aufrechterhalten werden. Privilegien sollten erst nach Abschluss des Berechtigungsprozesses gewährt werden.
- d) Die Entwicklung und Verwendung von Systemroutinen sollte gefördert werden, um zu verhindern, dass Benutzern Privilegien erteilt werden müssen.
- e) Privilegien sollten einer anderen Benutzerkennung als der, die für den normalen Geschäftsgebrauch verwendet wird, zugewiesen werden.

### 9.2.3 Verwaltung von Benutzerpasswörtern

Passwörter sind eine übliche Methode zur Bestätigung der Identität eines Benutzers vor dem Zugriff auf ein Informationssystem oder einen Informationsdienst. Die Zuteilung von Passwörtern sollte durch einen formalen Verwaltungsprozess kontrolliert werden, für den der folgende Ansatz gewählt werden sollte:

- a) Benutzer müssen eine Erklärung unterzeichnen, dass sie persönliche Passwörter und Passwörter von Arbeitsgruppen bis auf die Mitarbeiter in der Gruppe geheim halten (dieses könnte in die Anstellungsbedingungen aufgenommen werden, siehe 6.1.4);
- b) sofern Benutzer ihre eigenen Passwörter benutzen müssen, muss sichergestellt werden, dass sie zunächst ein sicheres vorläufiges Passwort erhalten, das sie sofort ändern müssen. Vorläufige Passwörter, die vergeben werden, wenn Benutzer ihr Passwort vergessen haben, sollten nur nach einer vorausgegangenen positiven Identifikation des Benutzers erteilt werden;
- c) vorläufige Passwörter müssen Benutzern auf sichere Art übergeben werden. Die Verwendung von Fremdunternehmen oder ungeschützten (Klartext) E-Mails sollte vermieden werden. Benutzer sollten den Empfang von Passwörtern bestätigen.

Passwörter sollten nie ungeschützt in einem Rechnersystem gespeichert werden (siehe 9.5.4).

Andere Techniken zur Identifikation und Authentisierung von Benutzern wie Biometrik, z.B. die Verifikation von Fingerabdrücken, die Verifikation von Unterschriften und die Verwendung von Hardware-Token, z.B. Chipkarten, sind verfügbar und sollten in entsprechenden Fällen in Betracht gezogen werden.

### 9.2.4 Überprüfung der Zugriffsrechte von Benutzern

Zur Aufrechterhaltung einer effektiven Kontrolle über den Zugriff auf Daten und Informationsdienste sollte das Management in regelmäßigen Abständen einen formalen Prozess zur Überprüfung der benutzereigenen Zugriffsrechte durchführen, so dass

- a) Benutzerzugriffsrechte in regelmäßigen Abständen (empfohlen wird ein Intervall von 6 Monaten) und nach jeder Änderung überprüft werden (siehe 9.2.1);
- b) Berechtigungen für spezielle privilegierte Zugriffsrechte (siehe 9.2.2) in kleineren Abständen überprüft werden; empfohlen wird ein Intervall von 3 Monaten;

- c) Privilegzuweisungen in regelmäßigen Abständen geprüft werden, um sicherzustellen, dass keine unberechtigten Privilegien erhalten wurden.

### 9.3 Verantwortung der Benutzer

Ziel: Verhinderung eines unberechtigten Benutzerzugriffs.

Die Zusammenarbeit berechtigter Benutzer ist eine Grundvoraussetzung für effektive Sicherheit. Benutzer sollten auf ihre Verantwortung für die Erhaltung effektiver Zugangskontrollen hingewiesen werden, insbesondere in Bezug auf den Passwortgebrauch und die Sicherheit der Benutzergeräte.

#### 9.3.1 Passwortgebrauch

Benutzer sollten bei der Wahl und beim Gebrauch von Passwörtern adäquate Sicherheitspraktiken befolgen.

Passwörter sind ein Mittel zur Bestätigung der Identität eines Benutzers und somit zur Feststellung der Zugriffsrechte für Geräte oder Dienste zur Informationsverarbeitung. Alle Benutzer sollten dazu angehalten werden,

- a) Passwörter geheim zu halten;
- b) Passwörter möglichst nicht schriftlich festzuhalten, es sei denn, sie können sicher aufbewahrt werden;
- c) Passwörter bei jedem Anzeichen einer möglichen Kompromittierung des Systems oder Passworts zu ändern;
- d) gute Passwörter mit mindestens sechs Zeichen auszuwählen, die
  - 1) leicht zu behalten sind;
  - 2) sich nicht auf etwas beziehen, was eine andere Person leicht erraten oder mittels personenbezogener Informationen herausfinden könnte, z.B. Namen, Telefonnummern und Geburtsdaten usw.;
  - 3) keine aufeinanderfolgenden identischen Zeichen beinhalten oder nur aus Zahlen oder nur aus Buchstaben bestehen;
- e) Passwörter in regelmäßigen Abständen oder basierend auf der Anzahl der Zugriffe zu ändern (Passwörter für Accounts mit Privilegien sollten häufiger als normale Passwörter geändert werden) und die wiederholte bzw. zyklische Verwendung alter Passwörter zu vermeiden;
- f) vorübergehende Passwörter beim ersten Anmelden zu ändern;
- g) Passwörter nicht als Teil eines automatischen Anmeldeprozesses zu verwenden, z.B. in einer Makro- oder Funktionstaste;
- h) keine individuellen Benutzerpasswörter mit anderen zu teilen.

Falls Benutzer auf mehrere Dienste oder Plattformen zugreifen müssen und mehrere Passwörter brauchen, sollte ihnen der Gebrauch eines einzigen guten Passwortes (siehe d)

Oben) für alle Dienste empfohlen werden, die ein akzeptables Maß an Schutz für gespeicherte Passwörter bieten.

### **9.3.2 Unbeaufsichtigte Benutzergeräte**

Benutzer sollten sicherstellen, dass unbeaufsichtigte Geräte entsprechend geschützt sind. Geräte in Benutzerbereichen, z.B. Arbeitsstationen oder Datei-Server, können einen spezifischen Schutz vor unberechtigtem Zugriff erfordern, wenn sie für einen längeren Zeitraum unbeaufsichtigt gelassen werden.

Alle Benutzer und Auftragnehmer sollten sowohl auf die Sicherheitsanforderungen und -verfahren zum Schutz unbeaufsichtigter Geräte als auch auf ihre Verantwortung für die Implementierung derartiger Schutzmaßnahmen hingewiesen werden. Benutzer sollten dazu angehalten werden,

- a) aktive Sitzungen zu schließen, wenn sie sie beendet haben, sofern diese nicht durch einen entsprechenden Sperrmechanismus, z.B. einen passwortgeschützten Bildschirmschoner, gesichert werden können;
- b) sich von Großrechnern abzumelden, wenn die Sitzung beendet ist (d.h. nicht einfach nur den PC oder das Terminal auszuschalten);
- c) PCs oder Terminals, wenn sie nicht benutzt werden, zum Schutz vor einer unberechtigten Benutzung mit einem Tastaturschloss oder eine entsprechende Maßnahme zu sichern, z.B. durch ein Passwort.

## **9.4 Netzzugriffskontrolle**

Ziel: Schutz von vernetzten Diensten.

Der Zugriff auf sowohl interne als auch externe vernetzte Dienste sollte kontrolliert werden.

Dies ist notwendig, damit sichergestellt werden kann, dass Benutzer, die Zugriff auf Netze und Netzdienste haben, nicht die Sicherheit dieser Netzdienste kompromittieren. Das wird mit Hilfe der folgenden Maßnahmen sichergestellt:

- a) entsprechende Schnittstellen zwischen dem Organisationsnetz und den Netzen anderer Organisationen oder öffentlichen Netzen;
- b) entsprechende Authentisierungsmechanismen für Benutzer und Geräte;
- c) Kontrolle des Benutzerzugriffs auf Informationsdienste.

### **9.4.1 Politik zur Benutzung von Netzdiensten**

Unsichere Verbindungen zu Netzdiensten können Auswirkungen auf die gesamte Organisation haben. Benutzern sollte der direkte Zugriff nur auf Dienste, deren Benutzung ihnen ausdrücklich gestattet wurde, ermöglicht werden. Diese Maßnahme ist besonders wichtig für Netzverbindungen mit sensitiven oder kritischen Geschäftsanwendungen oder mit Benutzern an risikogefährdeten Standorten, z.B. in öffentlichen oder externen Bereichen, die außerhalb der Sicherheitsverwaltung und des Kontrollbereichs der Organisation liegen.

Es sollte eine Politik zur Verwendung von Netzen und Netzdiensten formuliert werden. Sie sollte folgende Punkte abdecken:

- a) Netze und Netzdienste, auf die ein Zugriff gestattet ist;

- b) Berechtigungsverfahren zur Feststellung, wer auf welche Netze und Netzdienste zugreifen darf;
- c) Maßnahmen und Verfahren des Managements zum Schutz des Zugriffs auf Netzverbindungen und Netzdienste.

Diese Politik sollte mit der Geschäftszugangskontrollpolitik konsistent sein (siehe 9.1).

#### **9.4.2 Eingeschränkter Pfad**

Unter Umständen muss der Pfad vom Benutzerterminal zum Rechnerdienst kontrolliert werden. Netze sind so gestaltet, dass sie ein Höchstmaß an gemeinsamer Nutzung von Mitteln und Flexibilität beim Routing ermöglichen. Diese Eigenschaften können auch Gelegenheit zu unberechtigtem Zugriff auf Geschäftsanwendungen oder zu einer unberechtigten Nutzung der Informationsgeräte bieten. Durch die Einführung von Maßnahmen, die die Route zwischen einem Benutzerterminal und den Rechnerdiensten beschränken, für die ihr Benutzer zugriffsberechtigt ist, z.B. durch die Einrichtung eines eingeschränkten Pfads, können diese Risiken reduziert werden.

Ziel eines eingeschränkten Pfads ist es, zu verhindern, dass Benutzer Routen abseits der Route zwischen Benutzerterminal und den Diensten wählen, für die der Benutzer eine Zugriffsberechtigung hat.

Dies erfordert normalerweise die Implementierung einer Anzahl von Maßnahmen an verschiedenen Stellen der Route. Prinzipiell sollten die Routingoptionen an jedem Punkt des Netzes durch eine vorher bestimmte Wahl begrenzt werden.

Dazu gibt es folgende Beispiele:

- a) Zuweisung dedizierter Leitungen oder Telefonnummern;
- b) automatische Verbindung von Ports mit bestimmten Anwendungssystemen oder Sicherheits-Gateways;
- c) Begrenzung der Menü- und Untermenü-Optionen für einzelne Benutzer;
- d) Verhinderung eines unbegrenzten Roamings im Netz;
- e) Vorschrift für externe Netzbenutzer, die spezifizierten Anwendungssysteme und/oder Sicherheits-Gateways zu benutzen;
- f) aktive Kontrolle erlaubter Kommunikationen vom Absender zum Empfänger über Sicherheits-Gateways, z.B. Firewalls;
- g) Beschränkung des Netzzugriffs durch die Einrichtung getrennter logischer Domänen, z.B. virtuelle private Netze, für Benutzergruppen innerhalb der Organisation (siehe auch 9.4.6).

Die Anforderungen an einen eingeschränkten Pfad sollten auf der Politik zur Zugangskontrolle nach Geschäftsanforderungen beruhen (siehe 9.1).

#### **9.4.3 Benutzerauthentisierung für externe Verbindungen**

Externe Verbindungen bieten ein Potential für unberechtigten Zugriff auf Geschäftsinformationen, z.B. den Zugriff über Einwahlmethoden. Aus diesem Grund sollten Benutzer an anderen Standorten einer Authentisierung unterworfen werden. Es gibt verschiedene Methoden für eine Authentisierung, von denen

einige ein höheres Maß an Schutz bieten als andere. Zum Beispiel können Methoden, die auf der Verwendung von kryptographischen Verfahren beruhen, eine starke Authentisierung bieten. Es ist wichtig, das erforderliche Maß an Schutz anhand einer Risikoanalyse zu bestimmen. Dies wird für die Wahl einer entsprechenden Authentisierungsmethode benötigt.

Die Authentisierung von Benutzern an anderen Standorten kann beispielsweise durch die Verwendung von kryptographischen Verfahren, Hardware-Token oder eines Challenge/Response-Protokolls erreicht werden. Dedizierte private Leitungen oder eine Prüfeinrichtung für die Adresse des Netzbenutzers können ebenfalls benutzt werden, um Gewissheit über die Verbindungsquelle zu erhalten.

Rückrufverfahren und -maßnahmen, z.B. die Verwendung von Rückruf-Modems, können Schutz vor unberechtigten und ungewollten Verbindungen mit den Geräten zur Informationsverarbeitung in einer Organisation bieten. Diese Maßnahme authentisiert Benutzer, die versuchen, von entfernten Standorten eine Verbindung zum Organisationsnetz herzustellen. Wird diese Maßnahme benutzt, sollte eine Organisation keine Netzdienste mit Rufweiterleitung verwenden bzw. diese Funktionen deaktivieren, um Schwachstellen in Verbindung mit der Rufweiterleitung zu vermeiden. Es ist ebenfalls wichtig, innerhalb des Rückrufprozesses zu gewährleisten, dass die Verbindung seitens der Organisation tatsächlich unterbrochen wird. Ansonsten könnte der Benutzer am anderen Ende die Leitung offen halten und vorgeben, dass eine Rückrufverifikation stattgefunden hat. Rückrufverfahren und -maßnahmen sollten gründlich auf diese Möglichkeit hin getestet werden.

#### **9.4.4 Knoten-Authentisierung**

Eine Einrichtung für eine automatische Verbindung mit einem entfernten Rechner könnte einen Weg zu einem unberechtigten Zugriff auf eine Geschäftsanwendung bieten. Verbindungen mit entfernten Rechnersystemen sollten deshalb authentisiert werden. Dies ist besonders wichtig, wenn die Verbindung ein Netz benutzt, das außerhalb des Kontrollbereichs der Sicherheitsverwaltung der Organisation liegt. Einige Beispiele für Authentisierung und wie diese erreicht werden kann sind unter 9.4.3 oben beschrieben. Eine Knoten-Authentisierung kann als alternatives Mittel dienen, um Gruppen von Benutzern an anderen Standorten zu authentisieren, die mit einer sicheren gemeinsam genutzten Rechneinrichtung (siehe 9.4.3) verbunden sind.

#### **9.4.5 Schutz des Ferndiagnoseports**

Der Zugang zu Diagnoseports sollte streng überwacht werden. Viele Rechner und Kommunikationssysteme sind mit einer anwählbaren Ferndiagnosefunktion für den Gebrauch durch Wartungsingenieure ausgerüstet. Bei fehlendem Schutz stellen diese Diagnoseports einen Weg für einen unberechtigten Zugriff dar. Sie sollten deshalb mit einem entsprechenden Sicherheitsmechanismus geschützt werden, z.B. einem Tastaturschloss und einem Verfahren, das dafür sorgt, dass ein Zugang nur nach Vereinbarung zwischen dem Manager des Rechnerdienstes und dem den Zugang verlangenden Hardware-/Software-Supportpersonal möglich ist.

#### **9.4.6 Trennung in Netzwerken**

Mit der Entstehung von Geschäftspartnerschaften, die Bedarf an Querverbindungen oder der gemeinsamen Nutzung von Informationsverarbeitungs- und Netzeinrichtungen haben, nimmt die Erweiterung von Netzen über die traditionellen Grenzen der Organisation hinaus zu.

Derartige Erweiterungen könnten das Risiko unberechtigter Zugriffe auf bereits bestehende Informationssysteme, die das Netz benutzen, erhöhen. Einige dieser Systeme könnten aufgrund ihrer Sensitivität oder kritischen Natur Schutz vor anderen Benutzern des Netzes benötigen. Unter solchen Umständen sollte die Einführung von Maßnahmen innerhalb des Netzes in Betracht gezogen werden, die Gruppen von Informationsdiensten, Benutzern und Informationssystemen trennen.

Eine Methode zur Kontrolle der Sicherheit großer Netze besteht darin, die Netze in getrennte logische Netzdomänen aufzuteilen, z.B. interne und externe Netzdomänen einer Organisation, die jeweils durch eine definierte Sicherheitsgrenze geschützt sind. Eine derartige Sicherheitsgrenze kann durch die Installation eines sicheren Gateways zwischen den beiden Netzen, die vernetzt werden sollen, implementiert werden, um den Zugriff und Informationsfluss zwischen den beiden Domänen zu kontrollieren. Dieses Gateway sollte so konfiguriert sein, dass es den Verkehr zwischen diesen Domänen filtert (siehe 9.4.7 und 9.4.8) und unberechtigte Zugriffe in Übereinstimmung mit der Zugangskontrollpolitik der Organisation verhindert (siehe 9.1). Ein Beispiel für diesen Gateway-Typ ist das, was üblicherweise als Firewall bezeichnet wird.

Die Kriterien für die Trennung von Netzen in Domänen sollten auf der Zugangskontrollpolitik und den Zugriffsanforderungen beruhen (siehe 9.1) und außerdem die relativen Auswirkungen von Kosten und Leistungen der Integration einer geeigneten Netzrouting- oder Gatewaytechnologie berücksichtigen (siehe 9.4.7 und 9.4.8).

#### **9.4.7 Kontrolle der Netzverbindung**

Anforderungen für eine Zugriffskontrollpolitik gemeinsamer genutzter Netze, insbesondere jener, die über die Grenzen der Organisation hinausgehen, können die Einbeziehung von Maßnahmen zur Beschränkung der Verbindungskapazität der Benutzer erforderlich machen. Derartige Maßnahmen können durch Netz-Gateways implementiert werden, die den Verkehr mittels vordefinierter Tabellen oder Regeln filtern. Die angewendeten Beschränkungen sollten auf der Zugangspolitik und den Anforderungen der Geschäftsanwendungen beruhen (siehe 9.1) und entsprechend gewartet und aktualisiert werden.

Beispiele für Anwendungen, für die Beschränkungen implementiert werden sollten, sind:

- a) E-Mail;
- b) Datenübertragung in eine Richtung;
- c) Datenübertragung in beide Richtungen;
- d) interaktiver Zugriff;
- e) Tageszeit- oder datumsgebundener Netzzugriff.

#### **9.4.8 Netzrouting-Kontrolle**

Gemeinsame Netze, besonders jene, die sich über die Grenzen von Organisationen erstrecken, können die Einführung von Routing-Maßnahmen erfordern, um sicherzustellen, dass Rechnerverbindungen und Informationsflüsse nicht gegen die Zugangskontrollpolitik für Geschäftsanwendungen verstoßen (siehe 9.1). Diese Maßnahme ist häufig wichtig für Netze, die gemeinsam mit Benutzern von Fremdunternehmen genutzt werden.

Routing-Kontrollen sollten auf positiven Prüfmechanismen für die Quell- und Zieladresse beruhen. Die Übertragung von Netzadressen ist auch ein sehr nützlicher Mechanismus zur

Isolierung von Netzen und zur Verhinderung, dass sich Routen aus dem Netz einer Organisation in das Netz einer anderen Organisation ausbreiten. Er kann in Soft- oder Hardware implementiert werden. Die für die Implementierung verantwortliche Person sollte sich der Stärke des jeweils installierten Mechanismus bewusst sein.

#### **9.4.9 Sicherheit von Netzdiensten**

Es steht eine breite Palette öffentlicher oder privater Netzdienste zur Verfügung, von denen einige zusätzlichen Leistungen anbieten. Netzdienste können spezielle oder komplexe Sicherheitsmerkmale besitzen. Organisationen, die Netzdienste nutzen, sollten sicherstellen, dass eine klare Beschreibung der Sicherheitsattribute aller benutzten Dienste vorliegt.

### **9.5 Kontrolle des Betriebssystemzugriffs**

Ziel: Verhinderung von unberechtigten Rechnerzugriffen.

Zur Beschränkung des Zugriffs auf Rechnerressourcen sollten Sicherheitseinrichtungen auf der Betriebssystemebene verwendet werden. Diese Einrichtungen sollten zu folgendem in der Lage sein:

- a) Identifikation und Verifikation der Identität und, wenn nötig, des Terminals oder des Standorts jedes berechtigten Benutzers;
- b) Aufzeichnung erfolgreicher und fehlgeschlagener Systemzugriffe;
- c) Bereitstellung geeigneter Mittel zur Authentisierung; bei Verwendung eines Passwortverwaltungssystems sollte dieses gute Passwörter sicherstellen [siehe 9.3.1 d)];
- d) Beschränkung der Verbindungsdauer des Benutzers in entsprechenden Fällen.

Andere Zugriffskontrollmethoden wie z.B. Challenge/Response sind verfügbar, sofern sie auf der Basis des Geschäftsrisikos gerechtfertigt sind.

#### **9.5.1 Automatische Terminalidentifikation**

Eine automatische Terminalidentifikation sollte in Betracht gezogen werden, um die Verbindungen mit spezifischen Standorten und tragbaren Geräten zu authentisieren. Die automatische Terminalidentifikation ist eine Technik, die genutzt werden kann, wenn es wichtig ist, dass die Sitzung nur von einem bestimmten Standort oder Rechnerterminal aus gestartet werden kann. Eine Kennung im oder am Terminal kann benutzt werden, um Auskunft zu geben, ob dieses Terminal spezifische Transaktionen starten oder empfangen darf. Zur Erhaltung der Sicherheit der Terminalkennung kann es erforderlich sein, einen physischen Schutz für das Terminal zu verwenden. Zur Authentisierung von Benutzern können zudem eine Anzahl anderer Techniken eingesetzt werden (siehe 9.4.3).

#### **9.5.2 Anmeldeverfahren an Terminals**

Der Zugriff auf Informationsdienste sollte über ein sicheres Anmeldeverfahren möglich sein.

Das Anmeldeverfahren für ein Rechnersystem sollte derart gestaltet sein, dass die Gelegenheit zu einem unberechtigten Zugriff auf ein Mindestmaß beschränkt wird. Das Anmeldeverfahren sollte deshalb ein Minimum an Informationen über das System bekannt geben, um zu vermeiden, dass einem unberechtigten Benutzer unnötig Unterstützung gegeben wird. Ein gutes Anmeldeverfahren sollte

- a) keine System- oder Anwendungskennungen anzeigen, bevor der Anmeldevorgang erfolgreich beendet wurde;
  - b) einen allgemeinen Hinweis anzeigen, der davor warnt, dass der Rechnerzugriff nur für berechnigte Benutzer gestattet ist;
  - c) während des Anmeldeverfahrens keine Hilfsmeldungen anbieten, die einem unberechnigten Benutzer helfen könnten;
  - d) die Anmeldeinformationen erst nach Beendigung aller Eingabedaten bestätigen, falls ein Fehler auftritt, sollte das System nicht anzeigen, welcher Teil der Daten richtig oder falsch ist;
  - e) die Anzahl der erlaubten erfolglosen Anmeldeversuche beschränken (empfohlen sind drei Versuche) und folgendes in Erwägung ziehen:
    - 1) Aufzeichnung erfolgloser Versuche;
    - 2) Forcierung einer Zeitverzögerung, bevor weitere Anmeldeversuche erlaubt sind oder Ablehnung jeglicher weiterer Versuche ohne spezifische Berechnigung;
    - 3) Unterbrechung der Datenverbindungen;
- a) die für das Anmeldeverfahren erlaubte maximale und minimale Zeit begrenzen, bei Überschreitung sollte das System die Anmeldung abbrechen;
  - b) folgende Informationen nach Abschluss einer erfolgreichen Anmeldung anzeigen:
    - 1) Datum und Zeit der vorhergegangenen erfolgreichen Anmeldung;
    - 2) Angaben über erfolglose Anmeldeversuche seit der letzten erfolgreichen Anmeldung.

### 9.5.3 Benutzeridentifikation und -authentisierung

Alle Benutzer (inklusive technische Supportmitarbeiter wie z.B. Bediener, Netzwerk-Administratoren, Systemprogrammierer und Datenbank-Administratoren) sollten eine eindeutige Kennung (Benutzerkennung) für ihre persönliche und alleinige Benutzung haben, so dass Tätigkeiten nachträglich zur verantwortlichen Person zurückverfolgt werden können. Benutzerkennungen sollten keinerlei Auskunft über die Privilegien (siehe 9.2.2) des Benutzers geben, z.B. Manager, Aufsichtspersonal.

Unter außergewöhnlichen Umständen, wo es sich eindeutig um einen Vorteil für das Geschäft handelt, kann eine gemeinsame Benutzerkennung für eine Benutzergruppe oder für eine spezifische Arbeit benutzt werden. In solchen Fällen sollte die Genehmigung durch das Management dokumentiert werden. Zusätzliche Maßnahmen zur Aufrechterhaltung der Zurechenbarkeit können erforderlich sein.

Es gibt verschiedene Authentisierungsverfahren, die zur Untermauerung der vorgegebenen Identität eines Benutzers herangezogen werden können. Passwörter (siehe auch 9.3.1 und unten) sind eine sehr übliche Methode zur Identifikation und Authentisierung (I&A), die auf einem Geheimnis basiert, das nur dem Benutzer bekannt ist. Das Gleiche kann auch mit kryptographischen Mitteln und Authentisierungsprotokollen erreicht werden.

Objekte wie z.B. Memory-Token oder Smart-Cards, die Benutzer besitzen, können auch für die I&A verwendet werden. Auch biometrische Authentisierungstechnologien, die die einzigartigen Merkmale oder Attribute einer Person nutzen, können zur Authentisierung der

Identität einer Person herangezogen werden. Eine Kombination aus Technologien und Mechanismen, die sicher miteinander verbunden sind, führt zu einer stärkeren Authentisierung.

#### **9.5.4 Passwortverwaltungssystem**

Passwörter sind eines der wichtigsten Mittel zur Bestätigung der Zugriffsberechtigung eines Benutzers auf einen Rechnerdienst. Passwortverwaltungssysteme sollten eine effektive interaktive Einrichtung darstellen, die gute Passwörter gewährleistet (siehe 9.3.1 zu Richtlinien für den Gebrauch von Passwörtern).

Für einige Anwendungen ist die Zuteilung der Benutzerpasswörter durch eine unabhängige Autorität erforderlich. In den meisten Fällen werden die Passwörter von Benutzern gewählt und verwaltet. Ein gutes Passwortverwaltungssystem sollte

- a) zur Erhaltung der Zurechenbarkeit die Benutzung individueller Passwörter forcieren;
- b) in entsprechenden Fällen Benutzern erlauben, ihre eigenen Passwörter auszuwählen und zu ändern, und ein Bestätigungsverfahren integrieren, das die Korrektur von Eingabefehlern zulässt;
- c) eine Auswahl an guten Passwörtern, wie unter 9.3.1 beschrieben, forcieren;
- d) sofern Benutzer ihre eigenen Passwörter verwalten. Passwortänderungen wie unter 9.3.1 beschrieben forcieren;
- e) sofern Benutzer Passwörter auswählen, sie bei der ersten Anmeldung zum Ändern vorübergehender Passwörter zu zwingen (siehe 9.2.3);
- f) eine Aufzeichnung über vorherige Benutzerpasswörter führen, z.B. für die vergangenen 12 Monate, und eine Wiederverwendung verhindern;
- g) Passwörter bei der Eingabe nicht auf dem Bildschirm anzeigen;
- h) Passwortdateien und Anwendungssystemdaten getrennt speichern;
- i) Passwörter in verschlüsselter Form unter Verwendung eines Einweg-Verschlüsselungsalgorithmus speichern;
- j) vom Hersteller vorgegebene Passwörter nach Installation der Software ändern.

#### **9.5.5 Gebrauch von Systemdienstprogrammen**

Die meisten Rechnerinstallationen besitzen ein oder mehrere Systemdienstprogramme, die eventuell System- und Anwendungskontrollen außer Kraft setzen können. Es ist besonders wichtig, dass ihr Gebrauch eingeschränkt und streng kontrolliert wird. Folgende Maßnahmen sollten in Erwägung gezogen werden:

- a) Einsatz von Authentisierungsverfahren für Systemdienstprogramme;
- b) Trennung der Systemdienstprogramme von Anwendungssoftware;
- c) Begrenzung der Benutzung von Systemdienstprogrammen auf die minimal praktikable Anzahl von vertrauenswürdigen, berechtigten Benutzern;
- d) Berechtigung für den ad-hoc-Gebrauch von Systemdienstprogrammen;

- e) Begrenzung der Verfügbarkeit von Systemdienstprogrammen, z.B. für die Dauer einer genehmigten Änderung;
- f) Protokollieren jeder Benutzung von Systemdienstprogrammen;
- g) Definition und Dokumentation von Berechtigungsebenen für Systemdienstprogramme;
- h) Entfernung sämtlicher unnötiger Dienstprogramme auf Software-Basis und Systemsoftware.

### 9.5.6 Zwangsalarm für die Sicherheit der Benutzer

Die Bereitstellung eines Zwangsalarms sollte für Benutzer in Betracht gezogen werden, die Ziel einer Nötigung sein könnten. Die Entscheidung, ob ein Alarm dieser Art bereitgestellt wird, sollte auf einer Risikoanalyse beruhen. Es sollten definierte Zuständigkeiten und Verfahren für die Reaktion auf einen Zwangsalarm existieren.

### 9.5.7 Terminal-Timeout

Unbenutzte Terminals an Standorten mit erhöhtem Risiko, z.B. in öffentlichen oder externen Bereichen, die außerhalb der Sicherheitsverwaltung einer Organisation liegen, oder die risikogefährdeten Systemen dienen, sollten zur Verhinderung des Zugriffs durch unberechtigte Personen nach einer definierten Wartezeit abgeschaltet werden. Diese Timeout-Funktion sollte den Bildschirminhalt löschen und sowohl Anwendung als auch Netzsitzungen nach einer definierten Wartezeit schließen. Die Timeout-Verzögerung sollte die Sicherheitsrisiken des Bereichs und der Terminalbenutzer widerspiegeln.

Eine begrenzte Form einer Terminal-Timeout-Funktion kann für einige PCs angeboten werden. Sie löscht den Bildschirminhalt und verhindert einen unberechtigten Zugriff, schließt aber nicht die Anwendung oder die Netzsitzungen.

### 9.5.8 Begrenzung der Verbindungsdauer

Beschränkungen der Verbindungsdauer sollten zusätzliche Sicherheit für risikogefährdete Anwendungen bieten. Die Begrenzung des Zeitraums, während dem Verbindungen von Terminals mit Rechnerdiensten zugelassen sind, reduziert den Gelegenheitsspielraum für einen unberechtigten Zugriff. Eine derartige Maßnahme sollte für sensitive Rechneranwendungen erwogen werden, insbesondere für diejenigen, deren Terminals an Standorten mit hohem Risiko installiert sind, z.B. in öffentlichen oder externen Bereichen, die außerhalb der Sicherheitsverwaltung der Organisation liegen. Beispiele für Beschränkungen dieser Art sind:

- a) Verwendung vorher festgelegter Zeitsegmente, z.B. für Stapeldatei-Übertragungen, oder regelmäßige interaktive Sitzungen von kurzer Dauer;
- b) Beschränkung der Verbindungsdauer auf normale Bürostunden, falls kein Bedarf für Überstunden oder für verlängerten Betrieb, der über die Bürostunden hinausgeht, besteht.

## 9.6 Zugriffskontrolle für Anwendungen

Ziel: Verhinderung des unberechtigten Zugriffs auf Informationen, die sich in Informationssystemen befinden.

Für die Zugriffsbeschränkung innerhalb von Anwendungssystemen sollten Sicherheitsfunktionen verwendet werden.

Der logische Zugriff auf Software und Informationen sollte auf berechtigte Benutzer beschränkt werden. Anwendungssysteme sollten

- a) den Benutzerzugriff auf Informationen und Anwendungssystemfunktionen in Übereinstimmung mit einer definierten Geschäftszugriffspolitik kontrollieren;
- b) Schutz vor einem unberechtigten Zugriff auf Dienstprogramm- und Betriebssystemsoftware bieten, der System- oder Anwendungskontrollen außer Kraft setzen kann;
- c) die Sicherheit anderer Systeme, mit denen Informationsressourcen gemeinsam genutzt werden, nicht beeinträchtigen;
- d) nur der zuständigen Person, anderen ernannten berechtigten Personen oder definierten Benutzergruppen den Zugriff auf Informationen gewähren.

### 9.6.1 Beschränkung des Informationszugriffs

Benutzer von Anwendungssystemen, einschließlich Supportmitarbeiter, sollten nur in Übereinstimmung mit einer definierten Zugriffskontrollpolitik, die auf die einzelnen Anforderungen an Geschäftsanwendungen gegründet und konsistent mit der organisationseigenen Informationszugangspolitik ist, auf Informationen und Anwendungssystemfunktionen zugreifen dürfen (siehe 9.1). Die Anwendung der folgenden Maßnahmen sollte in Betracht gezogen werden, um die Anforderungen an die Zugriffsbeschränkung zu unterstützen:

- a) Bereitstellung von Menüs zur Kontrolle des Zugriffs auf die Anwendungssystemfunktionen;
- b) Beschränkung des Benutzerwissens hinsichtlich Informationen oder Anwendungssystemfunktionen, für die sie keine Zugriffsberechtigung haben, verbunden mit entsprechender Aufbereitung der Benutzerdokumentation;
- c) Kontrolle der Zugriffsrechte von Benutzern, z.B. Lesen, Schreiben, Löschen und Ausführen;
- d) Sicherstellung, dass Ausgaben von Anwendungssystemen, die sensitive Informationen verarbeiten, nur die Informationen enthalten, die für die Verwendung der Ausgabe relevant sind, und nur an berechtigte Terminals und Standorte geschickt werden. Außerdem sollen derartige Ausgaben in regelmäßigen Abständen überprüft werden, um sicherzustellen, dass redundante Informationen gelöscht werden.

### 9.6.2 Isolierung sensibler Systeme

Sensitive Systeme können eine dedizierte (isolierte) Rechnerumgebung erfordern. Einige Anwendungssysteme sind dermaßen sensitiv gegenüber einem potentiellen Verlust, dass sie eine spezielle Behandlung erfordern. Die Sensitivität kann bedeuten, dass das Anwendungssystem auf einem dedizierten Rechner laufen sollte, Ressourcen nur mit vertrauenswürdigen Anwendungssystemen gemeinsam nutzen sollte, oder frei von Begrenzungen sein sollte. Dazu gelten folgende Erwägungen:

- a) Die Sensitivität eines Anwendungssystems sollte genau festgestellt und von der für die Anwendung zuständigen Person dokumentiert werden (siehe 4.1.3).
- b) Wenn eine sensitive Anwendung in einer gemeinsam genutzten Umgebung laufen soll, sollten die Anwendungssysteme, mit denen es die Ressourcen gemeinsam nützt, identifiziert und mit der für die sensitive Anwendung zuständigen Person vereinbart werden.

## 9.7 Überwachung des Systemzugriffs und der Systembenutzung

Ziel: Aufdeckung unberechtigter Tätigkeiten.

Systeme sollten überwacht werden, um Abweichungen von der Zugriffskontrollpolitik aufzudecken und um aufzeichnungswürdige Ereignisse als Beweise für eventuelle Sicherheitsvorfälle festzuhalten.

Durch eine Überwachung des Systems kann die Effektivität getroffener Maßnahmen geprüft und die Konformität mit einem Zugriffspolitikmodell (siehe 9.1) verifiziert werden.

### 9.7.1 Protokollieren von Vorfällen

Auditprotokolle, in denen Ausnahmefälle und andere sicherheitsrelevante Vorfälle verzeichnet werden, sollten angefertigt und über einen vereinbarten Zeitraum aufbewahrt werden, um zukünftige Untersuchungen und die Überwachung der Zugriffskontrolle zu unterstützen. Auditprotokolle sollten auch folgende Elemente enthalten:

- a) Benutzerkennungen;
- b) Daten und Uhrzeiten von An- und Abmeldungen;
- c) Terminalkennung oder -Standort, soweit möglich;
- d) Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche;
- e) Aufzeichnungen über erfolgreiche und abgelehnte Daten- und andere Ressourcenzugriffsversuche.

Bestimmte Auditprotokolle müssen unter Umständen als Teil der Protokollaufbewahrungspolitik oder aufgrund von Anforderungen, Beweise zu sammeln, im Archiv abgelegt werden (siehe auch Abschnitt 12).

## 9.7.2 Kontrolle der Systembenutzung

### 9.7.2.1 Verfahren und Risikobereiche

Es sollten Kontrollverfahren für die Benutzung von Geräten zur Informationsverarbeitung eingerichtet werden. Derartige Verfahren sind erforderlich, um sicherzustellen, dass Benutzer nur Tätigkeiten ausführen, die ausdrücklich genehmigt wurden. Das erforderliche Kontrollniveau für einzelne Geräte sollte anhand einer Risikoanalyse bestimmt werden. Bereiche, die dabei berücksichtigt werden sollten, sind:

- a) berechtigter Zugriff und detaillierte Informationen wie z.B.:
  - 1) die Benutzererkennung;
  - 2) das Datum und die Uhrzeit wichtiger Ereignisse;
  - 3) die Arten von Ereignissen;
  - 4) die Dateien, auf die zugegriffen worden ist;
  - 5) das benutzte Programm/die benutzten Dienstprogramme;
- b) alle privilegierten Abläufe, wie z.B.:
  - 1) Benutzung eines Aufseher-Accounts;
  - 2) Systemstart und -stopp;
  - 3) Anschluss/Entfernung von Ein-/Ausgabegeräten;
- c) unberechtigte Zugriffsversuche wie z.B.:
  - 1) fehlgeschlagene Versuche;
  - 2) Verletzungen der Zugriffspolitik und Benachrichtigungen für Netz-Gateways und Firewalls;
  - 3) Warnungen von proprietären Systemen, die unberechtigtes Eindringen melden;
- d) Systemwarnungen oder -fehler wie z.B.:
  - 1) Konsolenwarnungen oder -meldungen;
  - 2) Systemprotokollausnahmen;
  - 3) Netzmanagementalarne.

### 9.7.2.2 Risikofaktoren

Das Ergebnis der Kontrolltätigkeiten sollte regelmäßig überprüft werden. Die Häufigkeit der Überprüfung sollte von den jeweiligen Risiken abhängig sein. Risikofaktoren, die dabei berücksichtigt werden sollten, sind:

- a) die Wichtigkeit der Anwendungsprozesse;
- b) der Wert, die Sensitivität oder kritische Natur der jeweiligen Informationen;
- c) die bisherige Erfahrung mit Infiltrierungen und Missbrauch des Systems;
- d) das Ausmaß der Systemvernetzung (insbesondere mit öffentlichen Netzen).

### 9.7.2.3 Protokollierung und Überprüfung von Vorfällen

Bei der Überprüfung eines Protokolls geht es darum, die Bedrohungen für das System und die Art und Weise, wie diese entstehen können, zu verstehen. Beispiele für Vorfälle, die unter Umständen im Rahmen von Sicherheitsvorfällen näher untersucht werden müssen, sind unter 9.7.1 beschrieben.

Systemprotokolle enthalten oft eine große Menge an Informationen, von denen viele für die Sicherheitskontrolle irrelevant sind. Um bedeutende Vorfälle zu Zwecken der Sicherheitskontrolle leichter identifizieren zu können, sollte in Erwägung gezogen werden, die relevanten Meldungstypen automatisch in ein zweites Protokoll kopieren zu lassen und/oder geeignete Systemdienstprogramme oder Audittools einzusetzen, um nach Dateien suchen zu können.

Bei der Zuweisung der Verantwortlichkeit für Protokollüberprüfungen sollte eine Trennung der Rollen zwischen den Personen in Erwägung gezogen werden, die die Überprüfung durchführen und denen, deren Tätigkeiten kontrolliert werden.

Besondere Aufmerksamkeit sollte der Sicherheit der Protokollfunktion zukommen, denn sie könnte bei Modifikation ein falsches Gefühl der Sicherheit schaffen. Maßnahmen sollten darauf ausgerichtet sein, vor unberechtigten Änderungen und Betriebsproblemen zu schützen wie z.B.:

- a) dem Abschalten der Protokollfunktion;
- b) Änderungen an den aufgezeichneten Meldungstypen;
- c) einer Bearbeitung oder Löschung von Protokolldateien;
- d) der Erschöpfung von Protokolldateimedien, wodurch entweder keine Ereignisse aufgezeichnet werden oder Ereignisse überschrieben werden.

### 9.7.3 Uhrensynchronisation

Die korrekte Einstellung von Rechneruhren ist wichtig, um die Genauigkeit von Auditprotokollen zu gewährleisten, die für Untersuchungen oder als Beweise vor Gericht oder in Disziplinarfällen benötigt werden können. Ungenaue Auditprotokolle können solche Untersuchungen behindern und die Glaubwürdigkeit derartiger Beweise beeinträchtigen.

Wo ein Rechner- oder Kommunikationsgerät über die Funktion einer Echtzeituhr verfügt, sollte diese auf eine vereinbarte Norm, z.B. universelle koordinierte Zeit (UCT) oder auf Standardortszeit eingestellt werden. Da einige Uhren bekanntlich mit der Zeit vor- oder nachgehen, sollte ein Verfahren existieren, das bedeutende Abweichungen erkennt und korrigiert.

## 9.8 Mobile Computing und Telearbeit

Ziel: Informationssicherheit bei Mobile Computing- und Telearbeit.

Der erforderliche Schutz sollte entsprechend der Risiken ausgelegt sein, die durch diese spezifischen Arbeitsweisen entstehen. Beim Mobile Computing sollten die Risiken bedacht werden, die durch das Arbeiten in einer ungeschützten Umgebung entstehen und entsprechende Sicherheitsmaßnahmen getroffen werden. Bei Telearbeit sollte die Organisation Sicherheitsmaßnahmen am Telearbeitsplatz einführen und dafür sorgen, dass entsprechende Vereinbarungen für diese Arbeitsweise getroffen worden sind.

### 9.8.1 Mobile Computing

Beim Einsatz von Mobile Computing-Geräten, z.B. Notebooks, Palmtops, Laptops und Handys, sollte besonders darauf geachtet werden, dass Geschäftsinformationen vor unberechtigtem Zugriff geschützt sind. Es sollte eine formale Sicherheitspolitik angewendet werden, in denen die Risiken bedacht werden, die beim Arbeiten mit Mobile Computing-Geräten, insbesondere in ungeschützten Umgebungen, entstehen. Zum Beispiel sollten in dieser Politik die Erfordernisse für physischen Schutz, Zugriffskontrollen, kryptographische Verfahren, Datensicherungen und Vorkehrungen zum Virenschutz enthalten sein. In dieser Politik sollten außerdem Regeln und Hinweise zum Anschluss von Mobilgeräten an Netzwerke und Richtlinien zur Benutzung dieser Geräte an öffentlichen Plätzen aufgenommen sein.

Vorsicht sollte beim Einsatz von Mobile Computing-Geräten an öffentlichen Plätzen, in Besprechungszimmern und anderen ungeschützten Bereichen außerhalb des Geländes der Organisation walten. Maßnahmen sollten getroffen worden sein, um einen unberechtigten Zugriff auf oder den Einblick in Informationen, die auf diesen Geräten gespeichert und verarbeitet worden sind, zu verhindern (z.B. mittels kryptographischer Verfahren, siehe 10.3).

Es ist wichtig, beim Einsatz von Geräten dieser Art an öffentlichen Plätzen darauf zu achten, dass Informationen nicht von unberechtigten Personen eingesehen werden können. Maßnahmen gegen infizierte Software sollten getroffen und ständig aktualisiert werden (siehe 8.3). Es sollten Geräte bereitstellen, mit denen Informationen schnell und einfach gesichert werden können. Diese Sicherungskopien sollten angemessen vor Diebstahl, Informationsverlust usw. geschützt werden.

Für die Benutzung von Mobilgeräten, die an Netzwerken angeschlossen sind, sollten geeignete Sicherheitsmaßnahmen getroffen werden. Ein Remote Access auf Geschäftsinformationen mit Mobile Computing-Geräten über ein öffentliches Netzwerk sollte nur nach erfolgreicher Identifikation und Authentisierung und bei vorhandenen Zugriffskontrollmechanismen stattfinden (siehe 9.4).

Mobile Computing-Geräte sollte außerdem physisch vor Diebstahl geschützt werden, insbesondere dann, wenn sie z.B. im Auto und anderen Verkehrsmitteln, Hotelzimmern, Konferenzzentren und an Treffpunkten liegengelassen werden. Geräte, auf denen wichtige, sensitive und/oder kritische Geschäftsinformationen abgespeichert sind, sollten nicht unbeaufsichtigt liegengelassen werden und sofern möglich physisch weggeschlossen werden oder mit speziellen Schlössern gesichert werden. Zu Einzelheiten bezüglich des physischen Schutzes von Mobilgeräten siehe 7.2.5.

Für Mitarbeiter, die mit Mobilgeräten arbeiten, sollte eine Schulung organisiert werden, um sie auf die zusätzlichen Risiken hinzuweisen, die durch diese Arbeitsweise entstehen, sowie auf die Maßnahmen, die implementiert werden sollten.

### **9.8.2 Telearbeit**

Bei Telearbeit wird Kommunikationstechnologie eingesetzt, die es Mitarbeitern erlaubt, von einem festen Standort außerhalb ihrer Organisation zu arbeiten. Am Telearbeitsplatz sollten geeignete Sicherheitsmaßnahmen eingeführt worden sein, z.B. Schutz vor dem Diebstahl von Geräten und Informationen, vor einer unberechtigten Offenlegung von Informationen, dem unberechtigten Remote Access auf interne Systeme der Organisation oder dem Missbrauch von Geräten. Es ist wichtig, dass die Telearbeit vom Management sowohl genehmigt als auch kontrolliert wird und dass geeignete Vereinbarungen für diese Arbeitsweise getroffen worden sind.

Organisationen sollten in Betracht ziehen, Sicherheitspolitiken, Verfahren und Nonnen zur Kontrolle der Telearbeit zu entwickeln. Organisationen sollten Telearbeit nur genehmigen, wenn sie überzeugt sind, dass angemessene Sicherheitsmaßnahmen vorhanden sind und dass diese mit der Sicherheitspolitik der Organisation im Einklang stehen, folgendes sollte bedacht werden:

- a) die vorhandene physische Sicherheit des Telearbeitsplatzes unter Berücksichtigung der physischen Sicherheit des Gebäudes und seiner Lage;
- b) die vorgeschlagene Umgebung des Telearbeitsplatzes;
- c) die Anforderungen an die Kommunikationssicherheit unter Berücksichtigung des Bedarfs für Remote Access auf die internen Systeme der Organisation, der Sensitivität der Informationen, auf die zugegriffen wird und die über die Kommunikationsverbindung übertragen werden und der Sensitivität des internen Systems;
- d) die Bedrohung eines unberechtigten Zugriffs auf Informationen oder Ressourcen durch andere Personen in der Wohnung/im Haus, z.B. Familienangehörige und Freunde.

Relevante Maßnahmen und Arrangements, die in Betracht gezogen werden müssen, sind:

- a) die Bereitstellung geeigneter Geräte und Möbel zur Aufbewahrung der Geräte für die Telearbeit;
- b) eine Definition der erlaubten Arbeit, der Arbeitsstunden, der Klassifizierung der Informationen, die u. U. gespeichert werden und interne Systeme und Dienste, auf die der Telearbeiter zugreifen darf;
- c) die Bereitstellung geeigneter Kommunikationsgeräte einschließlich Methoden zur Sicherung des Remote Access;
- d) die physische Sicherheit;
- e) die Regeln und Richtlinien in bezug auf den Zugang zu Geräten und Informationen durch Familienangehörige und Gäste;
- f) die Bereitstellung von Support und Wartung für Hardware und Software;
- g) die Back-up-Verfahren und Verfahren zur Sicherung der Aufrechterhaltung des Geschäftsbetriebs;

- h) die Audit- und Sicherheitsüberwachung;
- i) die Aufhebung von Berechtigungen, Zugriffsrechten und die Rückgabe der Geräte, wenn die Telearbeit beendet ist.

## **10 Systementwicklung und –Wartung**

### **10.1 Sicherheitsanforderungen an Systeme**

Ziel: Sicherheit in Informationssysteme einzubauen.

Dies umfasst die Infrastruktur, Geschäftsanwendungen und von Benutzern entwickelte Anwendungen. Der Entwurf und die Implementierung der Geschäftsprozesse, die die Anwendung oder den Dienst unterstützen, können für deren Sicherheit ausschlaggebend sein.

Vor der Entwicklung von Informationssystemen sollten Sicherheitsanforderungen identifiziert und vereinbart werden.

Alle Sicherheitsanforderungen, einschließlich des Bedarfs an Reserveplänen, sollten in der Anforderungsphase eines Projekts festgestellt und als Teil der gesamten Geschäftsbegründung für ein Informationssystem gerechtfertigt, vereinbart und dokumentiert werden.

#### **10.1.1 Analyse und Spezifikation der Sicherheitsanforderungen**

Aussagen über Geschäftsanforderungen für neue Systeme oder Verbesserungen für existierende Systeme sollten die Anforderungen für Maßnahmen spezifizieren. Bei diesen Spezifikationen sollten die automatisierten Maßnahmen, die in das System integriert werden sollen, und der Bedarf an unterstützenden manuellen Maßnahmen bedacht werden. Ähnliche Überlegungen sollten bei der Bewertung von Softwarepaketen für Geschäftsanwendungen angestellt werden. Sofern das Management es für sinnvoll hält, können auch Produkte genutzt werden, die unabhängig evaluiert und zertifiziert worden sind.

Sicherheitsanforderungen und -maßnahmen sollten den Geschäftswert der beteiligten Informationen und Werte reflektieren, sowie den potentiellen Schaden für das Geschäft, der durch das Fehlen oder Nichtvorhandensein von Sicherheit entstehen kann. Der Rahmen für die Analyse von Sicherheitsanforderungen und die Identifizierung von Maßnahmen zur Erfüllung dieser Anforderungen ist Risikoanalyse und Risikomanagement.

Maßnahmen, die in der Entwurfsphase integriert werden, können erheblich kostengünstiger implementiert und aufrecht erhalten werden als Maßnahmen, die während oder nach der Implementierung integriert werden.

## 10.2 Sicherheit in Anwendungssystemen

Ziel: Verhinderung von Verlust, Änderung oder Missbrauch von Benutzerdaten in Anwendungssystemen.

Angemessene Maßnahmen und Auditprotokolle oder Aktivitätsprotokolle sollten in der Entwurfsphase in Anwendungssysteme und in von Benutzern entworfenen Anwendungen integriert werden. Darin sollten auch die Validierung der Eingabedaten, der internen Verarbeitung und der Ausgabedaten enthalten sein.

Für Systeme, die sensitive, wertvolle oder kritische Organisationsbestände verarbeiten oder beeinflussen, können zusätzliche Maßnahmen erforderlich sein. Diese Maßnahmen sollten vor dem Hintergrund der Sicherheitsanforderungen und der Risikoanalyse festgelegt werden.

### 10.2.1 Validierung der Eingabedaten

Die Dateneingabe in Anwendungssystemen sollte validiert werden, um sicherzustellen, dass sie korrekt und passend ist. Geprüft werden sollten die Eingaben von Geschäftstransaktionen, konstanten Daten (Namen und Adressen, Kreditlimits, Kundennummern) und Parametertabellen (Verkaufspreise, Devisenkurse, Steuersätze). Folgende Maßnahmen sollten bedacht werden:

- a) doppelte Eingabe- oder andere Eingabeprüfungen zum Aufdecken der folgenden Fehler:
  - 1) Werte außerhalb des definierten oder sinnvollen Bereichs;
  - 2) ungültige Zeichen in Datenfeldern;
  - 3) fehlende oder unvollständige Daten;
  - 4) Überschreitung der oberen und unteren Grenzen für den Datenumfang;
  - 5) unberechtigte oder inkonsistente Kontrolldaten;
- b) periodische Nachprüfung des Inhalts der Schlüsselfelder oder Dateien zur Bestätigung ihrer Validität und Integrität;
- c) Inspektion von Ausdrucken eingehender Dokumente auf unberechtigte Änderungen an Eingabedaten (alle Änderungen in eingehenden Dokumenten sollten genehmigt werden);
- d) Verfahren für die Reaktion auf Validierungsfehler;
- e) Verfahren zum Prüfen der Plausibilität der Eingabedaten;
- f) Definition der Zuständigkeiten sämtlichen Personals, das am Prozess der Dateneingabe beteiligt ist.

### 10.2.2 Kontrolle der internen Verarbeitung

#### 10.2.2.1 Risikobereiche

Daten, die korrekt eingegeben wurden, können durch Verarbeitungsfehler oder mutwillig beschädigt werden. In Systeme sollten Validierungsprüfungen integriert werden, um derartige Verfälschungen zu erkennen. Der Entwurf der Anwendungen sollte sicherstellen, dass

Beschränkungen implementiert werden, die die Gefahr von Verarbeitungsfehlern, die letztlich zu einem Integritätsverlust führen, auf ein Minimum reduzieren. Spezifische Bereiche, die in diesem Zusammenhang zu beachten sind:

- a) die Benutzung und Stelle von Funktionen zum Hinzufügen und Löschen in Programmen, um Datenänderungen zu implementieren;
- b) Verfahren, um Programme daran zu hindern, in der falschen Reihenfolge oder nach einem Fehler bei der vorhergegangenen Verarbeitung zu laufen (siehe auch 8.1.1);
- c) Benutzung der richtigen Programme zur Rekonstruktion von Daten nach einem Fehler, um die richtige Verarbeitung der Daten zu gewährleisten.

### **10.2.2.2 Prüfungen und Kontrollen**

Die erforderlichen Maßnahmen sind von der Anwendungsart und den Auswirkungen der Datenverfälschung auf das Geschäft abhängig. Beispiele von Kontrollen, die integriert werden können, sind:

- a) Session- oder Batch-Kontrollen zur Abstimmung von Dateisalden nach Transaktionsaktualisierungen;
- b) Saldenkontrollen zur Prüfung von Anfangssalden gegen frühere Schlussalden, namentlich:
  - 1) Kontrollen von einem Lauf zum nächsten;
  - 2) Summe der Dateiaktualisierungen;
  - 3) Kontrollen von einem Programm zum nächsten;
- c) Validierung systemgenerierter Daten (siehe 10.2.1);
- d) Prüfung der Integrität von heruntergeladenen oder hochgeladenen Daten oder von Software zwischen zentralen und entfernten Rechnern (siehe 10.3.3);
- e) Prüfsumme von Listen und Dateien;
- f) Prüfungen zur Sicherstellung, dass Anwendungsprogramme zum richtigen Zeitpunkt laufen gelassen werden;
- g) Prüfungen zur Sicherstellung, dass Programme in der richtigen Reihenfolge laufen gelassen und bei Auftreten eines Fehlers beendet werden und dass die weitere Verarbeitung unterbrochen wird, bis das Problem gelöst ist.

### **10.2.3 Nachrichtenthauthentisierung**

Die Nachrichtenthauthentisierung ist eine Technik, die zur Erkennung unberechtigter Änderungen oder Verfälschungen von Inhalten einer übertragenen elektronischen Nachricht verwendet wird. Sie kann in Hard- oder Software implementiert werden, um eine physische Vorrichtung zur Nachrichtenthauthentisierung oder einen Softwarealgorithmus zu unterstützen.

Die Nachrichtenthauthentisierung sollte für Anwendungen in Betracht gezogen werden, bei denen eine Sicherheitsanforderung besteht, die Integrität des Nachrichteninhalts zu schützen, z.B. im elektronischen Zahlungsverkehr oder bei einem ähnlichen elektronischen Datenaustausch. Eine Analyse der Sicherheitsrisiken sollte durchgeführt werden, um zu bestimmen, ob eine Nachrichtenthauthentisierung erforderlich ist, und um die geeignetste Methode der Implementierung zu finden.

Die Nachrichtenauthentisierung ist nicht darauf ausgelegt, den Inhalt einer Nachricht vor einer unberechtigten Offenlegung zu schützen. Kryptographische Verfahren (siehe 10.3.2 und 10.3.3) können als ein geeignetes Werkzeug zur Implementierung der Nachrichtenauthentisierung eingesetzt werden.

### **10.2.4 Validierung der Ausgabedaten**

Datenausgaben aus einem Anwendungssystem sollten validiert werden, um sicherzustellen, dass die gespeicherten Informationen richtig verarbeitet wurden und den Umständen angemessen sind.

Typischerweise werden Systeme mit der Prämisse konstruiert, dass die Ausgabe nach einer angemessenen Validierung, Verifikation und Prüfung immer richtig ist. Das ist nicht immer der Fall. Die Validierung der Ausgabe kann aus folgenden Prüfungen und Kontrollen bestehen:

- a) Plausibilitätsprüfungen, um zu prüfen, ob die Ausgabedaten sinnvoll sind;
- b) Kontrollzählungen, um sicherzustellen, dass alle Daten verarbeitet wurden;
- c) Bereitstellung von genügend Informationen für einen Leser oder ein nachfolgendes Verarbeitungssystem, um die Genauigkeit, Vollständigkeit, Präzision und Klassifizierung der Informationen zu bestimmen;
- d) Verfahren für die Reaktion auf Ausgabevalidierungsprüfungen;
- e) Definition der Zuständigkeiten sämtlichen Personals, das am Prozess der Datenausgabe beteiligt ist.

## **10.3 Kryptographische Maßnahmen**

Ziel: Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen.

Kryptographische Systeme und Techniken sollten zum Schutz von Informationen eingesetzt werden, die als risikobehaftet eingestuft werden und für die andere Maßnahmen keinen angemessenen Schutz bieten.

### **10.3.1 Politik für den Einsatz kryptographischer Maßnahmen**

Ob eine kryptographische Lösung sinnvoll ist, sollte im Rahmen eines größeren Prozesses zur Beurteilung von Risiken und Auswahl von Maßnahmen entschieden werden. Es sollte eine Risikoanalyse durchgeführt werden, um den Schutzbedarf der Informationen zu bestimmen. Diese Analyse kann dann dazu verwendet werden, um zu bestimmen, ob kryptographische Maßnahmen sinnvoll sind, welche Art von Maßnahmen zur Anwendung kommen sollten und für welchen Zweck und welche Geschäftsprozesse sie eingesetzt werden sollten.

Eine Organisation sollte eine Politik für die Verwendung kryptographischer Maßnahmen zum Schutz ihrer Informationen entwickeln. Solch eine Politik ist notwendig, um Vorteile zu maximieren und Risiken zu minimieren, die durch den Einsatz von kryptographischen Verfahren entstehen, und um eine unsachgemäße oder falsche Verwendung auszuschließen. Bei der Entwicklung einer Politik für kryptographische Maßnahmen sollten die folgenden Punkte bedacht werden:

- a) die Strategie des Managements für den Einsatz kryptographischer Maßnahmen in der ganzen Organisation sowie allgemeine Prinzipien, mit denen Geschäftsinformationen geschützt werden sollten;

- b) das Schlüsselmanagement sowie Methoden, um verschlüsselte Informationen rekonstruieren zu können, wenn Schlüssel verloren, kompromittiert oder beschädigt werden;
- c) Rollen und Verantwortungsbereiche, z.B. wer trägt die Verantwortung für:
  - 1) die Implementierung der Politik;
  - 2) das Schlüsselmanagement;
- d) die Festlegung des angemessenen Niveaus für einen kryptographischen Schutz;
- e) die Anwendung der Normen für die effektive Implementierung in der ganzen Organisation (welche Lösung wird für welche Geschäftsprozesse verwendet).

### **10.3.2 Verschlüsselung**

Verschlüsselung ist eine kryptographische Technik, die zum Schutz vertraulicher Informationen eingesetzt werden kann. Sie sollte zum Schutz sensitiver oder kritischer Informationen in Betracht gezogen werden.

Basierend auf einer Risikoanalyse sollte das erforderliche Sicherheitsniveau unter Berücksichtigung des Typs und der Qualität des verwendeten Verschlüsselungsalgorithmus und der Länge der zu verwendenden kryptographischen Schlüssel identifiziert werden.

Bei der Implementierung der Kryptographie-Politik der Organisation sollten Regelungen und nationale Beschränkungen bedacht werden, die unter Umständen Auswirkungen auf die Verwendung von kryptographischen Verfahren in verschiedenen Teilen der Welt sowie auf Fragen zur grenzüberschreitenden Übertragung verschlüsselter Informationen haben. Zusätzlich sollte auch auf Beschränkungen bei der Aus- und Einfuhr von Verschlüsselungstechnik geachtet werden (siehe auch 12.1.6).

Professioneller Rat sollte eingeholt werden, um den geeigneten Schutzbedarf zu bestimmen, um geeignete Produkte auszuwählen, die den erforderlichen Schutz und die Implementierung eines sicheren Schlüsselmanagementsystems bieten (siehe auch 10.3.5). Zusätzlich müssen u. U. noch rechtliche Fragen in bezug auf Gesetze und Regelungen geklärt werden, die Auswirkungen auf den von der Organisation beabsichtigten Einsatz der Verschlüsselungstechnik haben könnten.

### **10.3.3 Digitale Signaturen**

Digitale Signaturen sind ein Mittel zum Schutz der Authentizität und Integrität elektronischer Dokumente. Sie können zum Beispiel im Electronic Commerce eingesetzt werden, wo verifiziert werden muss, wer ein elektronisches Dokument unterzeichnet hat und geprüft werden muss, ob der Inhalt des unterzeichneten Dokuments geändert worden ist.

Digitale Signaturen können für jedes beliebige Dokument, das in elektronischer Form vorliegt, angewandt werden, z.B. bei elektronischen Zahlungen, Überweisungen, Verträgen und Vereinbarungen. Digitale Signaturen können mittels einer Verschlüsselungstechnik implementiert werden, bei der ein Schlüsselpaar benutzt wird, das auf eindeutige Weise miteinander verbunden ist. Ein Schlüssel wird dabei für die Erstellung einer Signatur benutzt (der private Schlüssel) und der andere zur Überprüfung der Signatur (der öffentliche Schlüssel).

Die Vertraulichkeit des privaten Schlüssels sollte unbedingt gewährleistet werden. Dieser Schlüssel sollte geheimgehalten werden, da jede Person, die Zugang zu diesem Schlüssel hat, Dokumente wie z.B. Zahlungen und Verträge unterzeichnen kann und damit die Signatur des rechtlichen Besitzers dieses Schlüssels fälschen kann. Darüber hinaus ist es wichtig, die Integrität des öffentlichen Schlüssels zu schützen. Dieser Schutz ist durch die Verwendung eines Zertifikats (public key certificate) gegeben (siehe 10.3.5).

Bedacht werden müssen der Typ und die Qualität des verwendeten Signatur-Algorithmus und die Länge der zu verwendenden Schlüssel. Kryptographische Schlüssel für digitale Signaturen sollten verschieden von denjenigen Schlüsseln sein, die für die Verschlüsselung verwendet werden (siehe 10.3.2).

Bei der Verwendung von digitalen Signaturen sollten auch alle relevanten Gesetze bedacht werden, in denen die Bedingungen beschrieben sind, unter denen eine digitale Signatur rechtsverbindlich ist. Beim Electronic Commerce zum Beispiel ist es wichtig zu wissen, inwieweit digitale Signaturen rechtsgültig sind. In Fällen, in denen die Gesetzgebung unzureichend ist, ist es unter Umständen notwendig, zusätzlich zu den digitalen Signaturen verbindliche Verträge oder andere Vereinbarungen abzuschließen. Rechtlicher Rat sollte in bezug auf Gesetze und Regelungen eingeholt werden, die unter Umständen Auswirkungen auf die von der Organisation beabsichtigte Verwendung digitaler Signaturen haben.

#### **10.3.4 Nicht-Abstreitbarkeitservice**

Der Nicht-Abstreitbarkeitservice sollte in Fällen genutzt werden, in denen ein Streit über das Geschehen bzw. Nichtgeschehen eines Ereignisses oder einer Aktion geklärt werden muss, z.B. ein Streit über eine digitale Signatur auf einem elektronischen Vertrag oder einer Zahlung. Er kann dabei helfen, Beweismaterial darüber zu beschaffen, ob ein bestimmtes Ereignis oder eine Aktion stattgefunden hat, z.B. wenn abgestritten wird, dass eine elektronisch unterzeichnete Anweisung per E-Mail abgeschickt wurde. Dieser Service basiert auf einer Verwendung von Techniken für Verschlüsselung und digitale Signaturen (siehe auch 10.3.2 und 10.3.3).

### **10.3.5 Schlüsselmanagement**

#### **10.3.5.1 Schutz der kryptographischen Schlüssel**

Das Management von kryptographischen Schlüsseln ist für den effektiven Einsatz von kryptographischen Verfahren unerlässlich. Jede Kompromittierung oder Verlust von kryptographischen Schlüsseln kann zu einer Gefährdung der Vertraulichkeit, Authentizität und/oder Integrität von Informationen führen. Zur Unterstützung der beiden von der Organisation benutzten Arten von kryptographischen Verfahren (siehe unten) sollte ein Managementsystem eingerichtet sein.

- a) Secret-Key-Techniken (symmetrische Verfahren), bei denen zwei oder mehrere Personen den gleichen Schlüssel haben, der sowohl zum Ver- als auch zum Entschlüsseln von Informationen verwandt wird. Dieser Schlüssel darf nur den am Datenaustausch beteiligten Kommunikationspartnern bekannt sein, da jeder, der Zugang zu diesem Schlüssel hat, sämtliche Informationen, die mit diesem Schlüssel verschlüsselt wurden, entschlüsseln kann oder unberechtigt Informationen einfügen kann;
- b) Public-Key -Techniken (asymmetrische Verfahren), bei denen jeder Benutzer ein Schlüsselpaar erhält, und zwar einen öffentlichen Schlüssel (der jedem mitgeteilt werden darf) und einen privaten Schlüssel (der geheimgehalten werden muss).

Öffentliche-Schlüssel-Techniken können zur Verschlüsselung (siehe 10.3.2) und zum Erstellen digitaler Signaturen (siehe 10.3.3) verwendet werden.

Alle Schlüssel sollten vor Änderungen und Zerstörung geschützt werden, und geheime und private Schlüssel müssen vor unberechtigter Offenlegung geschützt werden. Zu diesem Zweck können auch kryptographische Verfahren eingesetzt werden. Geräte zum Generieren, Speichern und Archivieren von Schlüsseln sollten physisch geschützt werden.

### **10.3.5.2 Normen, Verfahren und Methoden**

Ein System zum Schlüsselmanagement sollte auf einem vereinbarten Satz aus Normen, Verfahren und sicheren Methoden basieren und folgende Punkte berücksichtigen:

- a) Schlüsselerzeugung für verschiedene kryptographische Systeme und Anwendungen;
- b) Erstellung und Erhalt von Public-Key-Zertifikaten;
- c) Ausgabe der Schlüssel an die jeweiligen Benutzer mit Anweisungen, wie der Schlüssel bei Erhalt aktiviert werden soll;
- d) Aufbewahrung von Schlüsseln und Anweisungen, wie berechnete Benutzer Zugang zu diesen Schlüsseln erhalten;
- e) Änderung oder Aktualisierung von Schlüsseln und Regeln, wann und wie Schlüssel geändert werden sollen;
- f) Umgang mit kompromittierten Schlüsseln;
- g) Sperrung von Schlüsseln und Anweisungen, wie Schlüssel gesperrt oder deaktiviert werden sollen, z.B. wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden);
- h) Wiederherstellung von Schlüsseln, die verlorengegangen oder beschädigt wurden, als Teil des Managements zur Aufrechterhaltung des Geschäftsbetriebs beschädigt wurden, z.B. um verschlüsselte Informationen zu rekonstruieren;
- i) Archivierung von Schlüsseln, z.B. für archivierte Informationen oder Back-ups;
- j) Zerstörung von Schlüsseln;
- k) Protokollierung und Überprüfung von Aktivitäten in Verbindung mit dem Schlüsselmanagement.

Um die Möglichkeit der Kompromittierung von Schlüsseln zu reduzieren, sollten die Schlüssel definierte Aktivierungs- und Deaktivierungszeitpunkte haben, so dass sie nur über einen begrenzten Zeitraum verwendet werden können. Dieser Zeitraum sollte von den Umständen abhängig gemacht werden, in denen die kryptographische Maßnahme eingesetzt wird, und von dem erkannten Risiko.

Verfahren zum Umgang mit rechtlichen Aufforderungen hinsichtlich des Zugangs zu kryptographischen Schlüsseln müssen u.U. bedacht werden. Zum Beispiel könnte der Fall eintreten, dass verschlüsselte Informationen für ein Gerichtsverfahren in unverschlüsselter Form zur Verfügung gestellt werden müssen. Neben der Ausgabe von sicher verwalteten geheimen und privaten Schlüsseln sollte auch der Schutz der öffentlichen Schlüssel bedacht werden. Es besteht die Bedrohung, dass eine Person

den öffentlichen Schlüssel eines Benutzers gegen seinen eigenen austauscht und auf diese Weise eine digitale Signatur fälscht. Diesem Problem wird durch die Verwendung eines öffentlichen-Schlüssel-Zertifikats begegnet. Diese Zertifikate sollten so angefertigt werden, dass der Besitzer des Schlüsselpaares (bestehend aus öffentlichem und privatem Schlüssel) durch die Informationen auf dem Zertifikat eindeutig als Besitzer des öffentlichen Schlüssels identifiziert wird. Es ist darum wichtig, dass dem Managementprozess, mit dem diese Zertifikate generiert werden, vollstes Vertrauen geschenkt werden kann. Dieser Prozeß wird normalerweise von einer Zertifizierungsstelle durchgeführt, bei der es sich um eine anerkannte Organisation mit geeigneten Maßnahmen, Kontrollen und Verfahren handeln sollte, der das nötige Vertrauen geschenkt werden kann.

Service-Vereinbarungen oder Verträge mit externen Providern kryptographischer Serviceleistungen, z.B. mit einer Zertifizierungsstelle, sollten Punkte wie Haftung, Zuverlässigkeit des Services und Reaktionszeiten für die Bereitstellung von Serviceleistungen abdecken (siehe 4.2.2).

#### **10.4 Sicherheit von Systemdateien**

Ziel: Gewährleistung, dass IT-Projekte und Supportaktivitäten auf sichere Art und Weise geführt werden.

Der Zugriff auf Systemdateien sollte kontrolliert werden.

Die Bewahrung der Systemintegrität sollte im Verantwortungsbereich der Benutzerfunktion oder der Entwicklungsgruppe liegen, der das Anwendungssystem oder die Software gehört.

##### **10.4.1 Kontrolle von Software in laufenden Systemen**

Die Implementierung von Software in laufenden Systemen sollte kontrolliert werden. Zur Minimierung des Risikos von Beschädigungen an laufenden Systemen sollten die folgenden Maßnahmen in Betracht gezogen werden:

- a) Die Aktualisierung der Programmbibliotheken in laufenden Systemen sollte nur von dem dazu ernannten Bibliothekar nach Erhalt einer entsprechenden Genehmigung vom Management durchgeführt werden (siehe 10.4.3).
- b) In laufenden Systemen sollte sich möglichst nur ausführbarer Code befinden.
- c) Ausführbarer Code sollte erst in ein laufendes System implementiert werden, nachdem der Beweis für erfolgreiche Tests und die Benutzerakzeptanz vorliegt, und nachdem die dazugehörigen Programmquellenbibliotheken aktualisiert wurden.
- d) Über alle Aktualisierungen von Programmbibliotheken in laufenden Systemen sollte ein Auditprotokoll geführt werden.
- e) Ältere Softwareversionen sollten als Reserve für den Notfall aufgehoben werden.

Software in laufenden Systemen, die vom Verkäufer bereitgestellt wird, sollte auf einem Level gewartet werden, der vom Hersteller unterstützt wird. Bei jeder Entscheidung für ein Upgrade zu einer neuen Version sollte die Sicherheit dieser Version, d.h. die Einführung von neuen Sicherheitsfunktionalitäten oder die Anzahl und Größe der Sicherheitsprobleme bei dieser Version, bedacht werden. Software-Patches sollten installiert werden, wenn sie dazu beitragen können, sicherheitsbezogene Schwächen zu beheben oder zu reduzieren.

Physischer und logischer Zugang sollte Herstellern, falls nötig, nur zu Supportzwecken und mit Genehmigung des Managements gewährt werden. Die Aktivitäten des Herstellers sollten überwacht werden.

#### **10.4.2 Schutz von Systemtestdaten**

Testdaten sollten geschützt und kontrolliert werden. System- und Übernahmetests benötigen gewöhnlich erhebliche Mengen an Testdaten, die den Daten im laufenden System möglichst nahe kommen. Die Verwendung von Datenbanken aus laufenden Systemen, die persönliche Informationen enthalten, sollte vermieden werden. Falls solche Informationen benutzt werden, sollten sie vor dem Gebrauch depersonalisiert werden. Die folgenden Kontrollen sollten verwendet werden, um Daten aus laufenden Systemen zu schützen, wenn sie für Testzwecke benutzt werden.

- a) Die Zugriffskontrollverfahren, die für laufende Anwendungssysteme gelten, sollten ebenfalls für Testanwendungen gelten.
- b) Für jeden Kopiervorgang von Informationen aus einem laufenden System in eine Testanwendung sollte eine zusätzliche Berechtigung notwendig sein.
- c) Informationen aus laufenden Systemen sollten von einer Testanwendung unmittelbar nach Vollendung des Tests gelöscht werden.
- d) Kopiervorgänge und die Benutzung von Informationen aus dem laufenden System sollten in einem Auditprotokoll aufgezeichnet werden.

#### **10.4.3 Zugriffskontrolle zur Programmquellenbibliothek**

Um die mögliche Beschädigung von Rechnerprogrammen zu reduzieren, sollte eine strenge Zugriffskontrolle für Programmquellenbibliotheken bestehen, die folgendermaßen beschaffen sein sollte (siehe auch 8.3):

- a) Nach Möglichkeit sollten sich Programmquellenbibliotheken nicht in laufenden Systemen befinden.
- b) Für jede Anwendung sollte ein Programmbibliothekar ernannt werden.
- c) IT-Support-Mitarbeiter sollten nicht über uneingeschränkten Zugriff auf Programmquellenbibliotheken verfügen.
- d) Programme, die gerade entwickelt oder gewartet werden, sollten sich nicht in laufenden Programmquellenbibliotheken befinden.
- e) Die Aktualisierung von Programmquellenbibliotheken und die Herausgabe von Programmquellen an Programmierer sollten nur durch den ernannten Bibliothekar nach Genehmigung des IT-Support-Managers für die Anwendung stattfinden.
- f) Programmlistings sollten in einer sicheren Umgebung aufbewahrt werden (siehe 8.6.4).
- g) Über sämtliche Zugriffe auf Programmquellenbibliotheken sollte ein Auditprotokoll geführt werden.
- h) Alte Versionen von Quellprogrammen sollten archiviert werden, mit exakter Angabe der genauen Daten und Zeiten ihres Betriebs, sowie sämtlicher Unterstützungssoftware, Ablaufsteuerung, sämtlichen Datendefinitionen und Verfahren.

- i) Die Wartung und das Kopieren von Programmquellenbibliotheken sollten strengen Änderungskontrollen unterworfen sein (siehe 10.4.1).

## 10.5 Sicherheit bei Entwicklungs- und Supportprozessen

Ziel: Sicherheit von Software und Informationen im Anwendungssystem erhalten. Projekt- und Supportumgebungen sollten streng kontrolliert werden.

Manager, die für Anwendungssysteme zuständig sind, sollten auch für die Sicherheit der Projekt- oder Supportumgebungen verantwortlich sein. Sie sollten dafür sorgen, dass alle vorgeschlagenen Systemveränderungen nochmals überdacht werden, um zu prüfen, ob sie die Sicherheit des Systems oder der Betriebsumgebung beeinträchtigen.

### 10.5.1 Änderungskontrollverfahren

Um die Beschädigung von Informationssystemen zu minimieren, sollten Implementierungen von Änderungen streng überwacht werden. Es sollten formale Änderungskontrollverfahren durchgesetzt werden. Sie sollten dafür sorgen, dass die Sicherheit und Überwachungsverfahren nicht kompromittiert werden, dass Supportprogrammierer nur auf diejenigen Systemteile Zugriff erhalten, die für ihre Arbeit nötig sind, und dass eine formale Übereinkunft und Zustimmung für jede Änderung erhalten werden. Eine Änderung der Anwendungssoftware kann Auswirkungen auf die gesamte Rechnerbetriebsumgebung haben. Sofern praktikierbar sollten Anwendungs- und ablaufspezifische Änderungskontrollverfahren integriert werden (siehe auch 8.1.2). Dieser Prüfvorgang sollte folgende Punkte beinhalten:

- a) Führen eines Verzeichnisses vereinbarter Berechtigungsebenen;
- b) Sicherstellung, dass Änderungen von berechtigten Benutzern eingereicht werden;
- c) Nachprüfen der Maßnahmen und Integritätsverfahren, um sicherzustellen, dass sie nicht durch die Veränderungen kompromittiert werden;
- d) Identifikation aller Software, Informationen, Datenbanken und Hardware, die Zusatzänderungen erfordern;
- e) Einholen der formalen Zustimmung für detaillierte Vorschläge vor Beginn der Arbeit;
- f) Sicherstellung vor der Implementierung, dass Änderungen von den berechtigten Benutzern akzeptiert werden;
- g) Sicherstellung, dass die Implementierung so durchgeführt wird, dass der Geschäftsablauf nur minimal gestört wird;
- h) Sicherstellung, dass die Systemdokumentation nach Abschluss jeder Änderung aktualisiert wird, und dass die alte Dokumentation archiviert oder entsorgt wird;
- i) Aufrechterhaltung einer Versionskontrolle für alle Softwareaktualisierungen;
- j) Führung eines Auditprotokolls mit sämtlichen Änderungsforderungen;
- k) Sicherstellung, dass die Betriebsdokumentation (siehe 8.1.1) und Benutzerverfahren entsprechend abgeändert werden;
- l) Sicherstellung, dass die Implementierung der Änderungen zum richtigen Zeitpunkt stattfindet und nicht die betroffenen Geschäftsprozesse stört.

Viele Organisationen verfügen über eine eigene Umgebung, in der Benutzer neue Software testen und die von den Entwicklungs- und Produktionsumgebungen komplett getrennt ist. Dadurch kann neue Software kontrolliert werden, und es wird ein zusätzlicher Schutz für Informationen in laufenden Systemen geboten, die für Testzwecke eingesetzt werden.

### **10.5.2 Technische Beurteilung der Änderungen am Betriebssystem**

Von Zeit zu Zeit ist es erforderlich, das Betriebssystem zu ändern, z.B. um eine neue Software-Version oder Patches zu installieren. Nach Änderungen sollten die Anwendungssysteme neu überprüft und getestet werden, um sicherzustellen, dass dadurch weder der Betrieb noch die Sicherheit beeinträchtigt worden sind. Dieser Prüfvorgang sollte folgende Punkte abdecken:

- a) Prüfung der Anwendungskontroll- und Integritätsverfahren, damit sichergestellt wird, dass diese nicht durch die Betriebssystemänderungen beeinträchtigt wurden;
- b) Sicherstellung, dass der jährliche Supportplan und das Jahresbudget durch Betriebssystemänderungen bedingte Überprüfungen und Systemtests mit einbezieht;
- c) Sicherstellung, dass Benachrichtigungen über Betriebssystemänderungen rechtzeitig zur Verfügung stehen, damit entsprechende Überprüfungen vor der Implementierung stattfinden können;
- d) Sicherstellung, dass die Pläne zur Aufrechterhaltung des Geschäftsbetriebs (siehe Abschnitt 11) entsprechend abgeändert werden.

### **10.5.3 Beschränkungen für Änderungen an Softwarepaketen**

Von Änderungen an Softwarepaketen sollte abgeraten werden. Soweit möglich und praktikierbar sollten Softwarepakete wie gekauft und ohne Änderungen benutzt werden. Wenn die Änderung eines Softwarepakets als unumgänglich betrachtet wird, sollten folgende Punkte bedacht werden:

- a) das Risiko der Kompromittierung eingebauter Maßnahmen und Integritätsprozesse;
- b) die Frage, ob vom Verkäufer eine Zustimmung eingeholt werden sollte;
- c) die Möglichkeit, die nötigen Änderungen vom Verkäufer als Standard-Programmaktualisierungen zu bekommen;
- d) die Auswirkungen, wenn die Organisation aufgrund der Änderungen für die zukünftige Wartung der Software zuständig wird.

Falls Änderungen unerlässlich erscheinen, sollte die Originalsoftware aufgehoben und die Änderungen an einer deutlich gekennzeichneten Kopie durchgeführt werden. Alle Änderungen sollten in vollem Umfang getestet und dokumentiert werden, so dass sie bei Bedarf an zukünftigen Softwareaktualisierungen erneut vorgenommen werden können.

#### 10.5.4 Verdeckte Kanäle und trojanischer Code

Ein verdeckter Kanal kann Informationen auf indirekten und obskuren Wegen freilegen. Aktiviert werden kann er u.U. durch die Änderung eines Parameters, auf den sowohl sichere als auch unsichere Komponenten eines Rechensystems zugreifen können, oder durch die Einbettung von Informationen in einen Datenstrom. Der trojanische Code ist so programmiert, dass er ein System in einer Weise beeinflusst, die nicht erlaubt ist, sich nicht sofort bemerkbar macht und auch nicht vom Empfänger oder Benutzer des Programms gebraucht wird. Verdeckte Kanäle und der trojanische Code treten selten durch Zufall auf. Sofern Sorge bezüglich verdeckter Kanäle oder trojanischen Codes besteht, sollten folgende Punkte beachtet werden:

- a) Programme nur von namhaften Quellen kaufen;
- b) Programme in Quellcode kaufen, so dass der Code überprüft werden kann;
- c) evaluierte Produkte benutzen;
- d) den gesamten Quellcode vor Einsatz des Programms inspizieren;
- e) Zugriff zum Code und Veränderungen des Codes nach der Programminstallation kontrollieren;
- f) nur Mitarbeiter, denen voll vertraut werden kann, an wichtigen System arbeiten lassen.

#### 10.5.5 Softwareentwicklung außerhalb der Organisation (Outsourcing)

Beim Outsourcen der Softwareentwicklung sollten die folgenden Punkte bedacht werden:

- a) Lizenzvereinbarungen, Code-Eigentum und intellektuelle Eigentumsrechte (siehe 12.1.2);
- b) Zertifizierung der Qualität und Genauigkeit der ausgeführten Arbeit;
- c) Treuhandverträge für den Fall des Versagens Dritter;
- d) Zugriffsrechte für die Prüfung der Qualität und der Genauigkeit der ausgeführten Arbeit;
- e) vertragliche Forderungen für die Qualität des Codes;
- f) Tests vor der Installation zur Suche nach trojanischem Code.

## 11 Management des kontinuierlichen Geschäftsbetriebs

### 11.1 Aspekte zur Aufrechterhaltung des Geschäftsbetriebs

Ziel: Einleitung von Maßnahmen gegen Unterbrechungen von Geschäftsaktivitäten und Schutz der kritischen Geschäftsprozesse vor den Auswirkungen großer Ausfälle oder Katastrophen.

Ein Prozess für das Management des kontinuierlichen Geschäftsbetriebs sollte implementiert werden, um Störungen durch Katastrophen und Sicherheitsausfälle (die z.B. Folge von Naturkatastrophen, Unfällen, Geräteausfällen und mutwilligen Beschädigungen sein können) durch eine Kombination aus vorsorglichen und wiederherstellenden Kontrollen auf ein akzeptables Maß zu reduzieren.

Die Folgen von Katastrophen, Sicherheitsausfällen und dem Verlust von Diensten sollten analysiert werden. Notfallpläne sollten entwickelt und implementiert werden, um sicherzustellen, dass Geschäftsprozesse in der erforderlichen Zeit wiederhergestellt werden können. Diese Pläne sollten aufbewahrt und einstudiert werden, damit sie zu einem integralen Bestandteil aller anderen Managementprozesse werden.

Zum Management des kontinuierlichen Geschäftsbetriebs gehören auch Maßnahmen zur Identifizierung und Reduzierung von Risiken, zur Begrenzung der Folgen von Vorfällen, durch die Schäden entstehen können, und die Garantie, dass grundlegende Abläufe schnell wieder aufgenommen werden können.

#### 11.1.1 Prozeß für das Management des kontinuierlichen Geschäftsbetriebs

Organisationsweit sollte ein verwalteter Prozess für die Entwicklung und Aufrechterhaltung der Geschäftsbetriebs vorhanden sein. Er sollte die folgenden Hauptelemente des Managements des kontinuierlichen Geschäftsbetriebs vereinen:

- a) Verständnis der Risiken, der die Organisation ausgesetzt ist, und ihrer Wahrscheinlichkeit und Auswirkungen, sowie eine Identifizierung und Priorisierung kritischer Geschäftsprozesse;
- b) Verständnis der wahrscheinlichen Auswirkungen auf das Geschäft durch Unterbrechungen (es ist wichtig, dass Lösungen für kleinere und große Vorfälle gefunden werden, durch die die Existenzfähigkeit der Organisation bedroht werden könnte) und Aufstellung der Unternehmensziele für die Geräte zur Verarbeitung von Information;
- c) Erwägung, eine geeignete Versicherung abzuschließen, die Teil des Prozesses für die Aufrechterhaltung des Geschäftsbetriebs sein könnte;
- d) Formulierung und Dokumentation einer Strategie für die Aufrechterhaltung des Geschäftsbetriebs, die mit den vereinbarten Unternehmenszielen und -Prioritäten übereinstimmt;
- e) Formulierung und Dokumentation von Plänen für die Aufrechterhaltung des Geschäftsbetriebs in Übereinstimmung mit der vereinbarten Strategie;
- f) regelmäßige Tests und Überarbeitungen der vorhandenen Pläne und Prozesse;

- g) Sicherstellung, dass das Management des kontinuierlichen Geschäftsbetriebs in die Prozesse und Strukturen der Organisation integriert wird. Die Verantwortung für die Koordinierung des Prozesses für das Management des kontinuierlichen Geschäftsbetriebs sollte auf eine angemessene Ebene in der Organisation übertragen werden, z.B. auf das Informationssicherheitsforum (siehe 4.1.1).

### **11.1.2 Aufrechterhaltung des Geschäftsbetriebs und Auswirkungsanalyse**

Die Aufrechterhaltung des Geschäftsbetriebs sollte mit der Identifizierung von Ereignissen beginnen, die zu Unterbrechungen von Geschäftsprozessen, z.B. Geräteausfälle, Überschwemmungen und Brand, führen können. Daran sollte sich eine Risikoanalyse anschließen, um die Auswirkungen dieser Unterbrechungen (sowohl hinsichtlich des Schadensausmaßes als auch des Wiederherstellungszeitraums) zu ermitteln.

Beide Tätigkeiten sollten unter vollständiger Einbeziehung der für die Geschäftsressourcen und -prozesse zuständigen Personen durchgeführt werden. Diese Analyse berücksichtigt sämtliche Geschäftsprozesse und ist nicht auf die Geräte zur Informationsverarbeitung beschränkt.

Je nach den Ergebnissen der Risikoanalyse sollte ein strategischer Plan entwickelt werden, um den Gesamtansatz zur Aufrechterhaltung des Geschäftsbetriebs festzulegen. Sobald dieser Plan erstellt ist, sollte er vom Management gebilligt werden.

### **11.1.3 Verfassen und Implementieren von Plänen zur Aufrechterhaltung des Geschäftsbetriebs**

Es sollten Pläne zur Aufrechterhaltung oder Wiederherstellung von Geschäftsabläufen nach einer Unterbrechung oder dem Ausfall kritischer Geschäftsprozesse innerhalb des geforderten Zeitrahmens entwickelt werden. Im Planungsprozess zur Aufrechterhaltung des Geschäftsbetriebs sollten folgende Elemente berücksichtigt werden:

- a) Identifikation und Vereinbarung aller Verantwortlichkeiten und Verfahren im Notfall;
- b) Implementierung von Verfahren im Notfall, um eine Wiederherstellung innerhalb des geforderten Zeitrahmens zu ermöglichen, besondere Aufmerksamkeit muss der Analyse externer Geschäftsabhängigkeiten und den vorhandenen Verträgen zukommen;
- c) Dokumentation vereinbarter Verfahren und Prozesse;
- d) entsprechende Schulungen für Mitarbeiter in den vereinbarten Verfahren und Prozessen für den Notfall einschließlich des Krisenmanagements;
- e) Testen und Aktualisierung der Pläne.

Der Planungsprozess sollte sich auf die erforderlichen Geschäftsziele konzentrieren, z.B. die Wiederherstellung spezifischer Dienste für Kunden in einem annehmbaren Zeitraum. Es sollten die Dienste und Ressourcen, die dieses ermöglichen, berücksichtigt werden, einschließlich der Mitarbeiterbesetzung, Ressourcen, die sich nicht auf die Verarbeitung von Informationen beziehen, sowie Reservemaßnahmen für Geräte zur Informationsverarbeitung.

### **11.1.4 Rahmen für die Pläne zur Aufrechterhaltung des Geschäftsbetriebs**

Ein Rahmen für Pläne zur Aufrechterhaltung des Geschäftsbetriebs sollte existieren und aufrechterhalten werden, damit die Konsistenz aller Pläne gewährleistet wird, und damit

Prioritäten für das Testen und das Aufrechterhalten der Pläne gesetzt werden. Jeder Plan zur Aufrechterhaltung des Geschäftsbetriebs sollte die Bedingungen für sein Inkrafttreten klar spezifizieren und die einzelnen Personen, die für die Ausführung jeder Komponente des Plans verantwortlich sind, angeben. Wenn neue Anforderungen identifiziert werden, sollten etablierte Verfahren für den Notfall, z.B. Evakuierungspläne oder bestehende Reservemaßnahmen, entsprechend abgeändert werden.

In einem Rahmen für die Pläne zur Aufrechterhaltung des Geschäftsbetriebs sollten folgende Elemente berücksichtigt werden:

- a) die Bedingungen zum Inkrafttreten des Plans, die den zu befolgenden Prozess beschreiben (Analyse der Situation, beteiligte Personen usw.), bevor jeder Plan in Kraft tritt;
- b) Verfahren für den Notfall, welche die Tätigkeiten beschreiben, die nach einem Vorfall zu ergreifen sind, bei dem Geschäftsabläufe und/oder Menschenleben gefährdet werden, dies sollte Arrangements für das PR-Management und eine effektive Zusammenarbeit mit den entsprechenden öffentlichen Behörden einschließen, z.B. der Polizei, Feuerwehr und Bezirksregierung;
- c) Reservemaßnahmen, welche die Tätigkeiten beschreiben, die zu ergreifen sind, um wichtige Geschäftstätigkeiten oder unterstützende Dienste zu alternativen vorübergehenden Standorten umzusiedeln, und um Geschäftsprozesse innerhalb des geforderten Zeitrahmens wieder zum Laufen zu bringen;
- d) Wiederaufnahmeverfahren, welche die Maßnahmen beschreiben, die für eine Rückkehr zum normalen Geschäftsbetrieb ergriffen werden müssen;
- e) ein Wartungsplan, welcher spezifiziert, wie und wann der Plan getestet wird, und den Prozeß zur Aufrechterhaltung des Plans;
- f) Maßnahmen für ein besseres Sicherheitsbewusstsein und Schulungen zum Verständnis der Prozesse zur Aufrechterhaltung des Geschäftsbetriebs und zur Sicherstellung, dass die Prozesse weiterhin effektiv sind;
- g) die Verantwortlichkeiten einzelner Personen mit einer Beschreibung, wer für die Ausführung welcher Komponente des Plans verantwortlich ist; Vertreter sollten je nach Bedarf ernannt werden.

Für jeden Plan sollte es eine spezifische Person geben, die zuständig ist. Verfahren im Notfall, manuelle Reservepläne und Wiederaufnahmepläne sollten innerhalb des Verantwortungsbereichs der für die entsprechenden beteiligten Geschäftsressourcen oder -prozesse zuständigen Personen liegen. Bei Reservemaßnahmen für alternative technische Dienste, wie z.B. Geräte zur Informationsverarbeitung und zur Kommunikation, sollte die Verantwortung in der Regel bei den Diensteanbietern liegen.

### **11.1.5 Testen, Aufrechterhaltung und erneute Analyse von Plänen zur Gewährleistung des kontinuierlichen Geschäftsbetriebs**

#### **11.1.5.1 Testen der Pläne**

Pläne zur Aufrechterhaltung des Geschäftsbetriebs können beim Testen oft aufgrund falscher Annahmen, Versehen oder Veränderungen von Geräten oder Personal versagen. Sie sollten deshalb regelmäßig getestet werden, um ihre Aktualität und Effektivität sicherzustellen. Derartige Tests sollten auch sicherstellen, dass alle Mitglieder des Wiederherstellungsteams und andere relevante Mitarbeiter wissen, dass es diese Pläne gibt.

Der Testplan für die Pläne zur Aufrechterhaltung des Geschäftsbetriebs sollte angeben, wie und wann jedes Element jedes Plans getestet werden sollte. Es wird empfohlen, die einzelnen Komponenten der Pläne häufig zu testen. Zur Sicherstellung, dass die Pläne im Ernstfall funktionieren, sollten verschiedene Techniken benutzt werden. Diese sollten folgende Punkte enthalten:

- a) Table-top-Tests verschiedener Szenarien (zur Besprechung der Wiederherstellungsmaßnahmen für den Geschäftsbetrieb unter Verwendung beispielhafter Unterbrechungen);
- b) Simulationen (insbesondere zur Schulung von Personal in ihren Rollen nach einem Vorfall/im Krisenmanagement);
- c) technische Wiederherstellungstests (zur Sicherstellung, dass Informationssysteme effektiv wiederhergestellt werden können);
- d) Wiederherstellungstests an einem alternativen Standort (Ablauf von Geschäftsprozessen parallel mit Wiederherstellungsabläufen an einem anderen Standort als dem Hauptstandort);
- e) Tests der Geräte und Dienste von Diensteanbietern (zur Sicherstellung, dass Lieferungen von Leistungen und Produkten die vertraglichen Verpflichtungen erfüllen werden);
- f) vollständige Übungen (zum Testen, dass die Organisation, das Personal, die Ausrüstung, Geräte und Prozesse mit Unterbrechungen umgehen können).

Die Techniken können von jeder Organisation genutzt werden und sollten die Art des spezifischen Wiederherstellungsplans widerspiegeln.

#### **11.1.5.2 Aufrechterhaltung und erneute Analyse der Pläne**

Pläne zur Aufrechterhaltung des Geschäftsbetriebs sollten regelmäßig überprüft und aktualisiert werden, um ihre kontinuierliche Effektivität sicherzustellen. Verfahren sollten innerhalb des organisationsweiten Programms für das Management von Veränderungen festgelegt werden, um sicherzustellen, dass auf Angelegenheiten in bezug auf die Aufrechterhaltung des Geschäftsbetriebs entsprechend reagiert wird.

Es sollten Verantwortungen für regelmäßige Überprüfungen jedes Plans zur Aufrechterhaltung des Geschäftsbetriebs zugeteilt werden. Der Identifikation von Änderungen in Geschäftsarrangements, die noch nicht in den Plänen zur Aufrechterhaltung des Geschäftsbetriebs reflektiert sind, sollte eine entsprechende Aktualisierung des Plans folgen. Dieser formale Änderungskontrollprozess sollte sicherstellen, dass die aktualisierten Pläne verteilt und durch regelmäßige Überprüfungen des vollständigen Plans unterstützt werden.

Beispiele für Situationen, in denen Pläne unter Umständen aktualisiert werden müssen, sind z.B. die Akquisition neuer Geräte oder die Aktualisierung von Betriebssystemen und Änderungen

- a) beim Personal;
- b) bei Adressen oder Telefonnummern;
- c) bei der Geschäftsstrategie;

- d) beim Standort, bei Geräten und Ressourcen;
- e) in der Gesetzgebung;
- f) bei Auftragnehmern, Lieferanten und wichtigen Kunden;
- g) bei Prozessen oder neuen/aus dem Betrieb genommenen Prozessen;
- h) beim Risiko (betrieblich und finanziell).

## **12 Einhaltung der Verpflichtungen**

### **12.1 Einhaltung gesetzlicher Verpflichtungen**

Ziel: Vermeidung von Verletzungen jeglicher Gesetze des Straf- oder Zivilrechts, gesetzlicher, behördlicher oder vertraglicher Verpflichtungen und jeglicher Sicherheitsanforderungen.

Die Entwicklung, der Betrieb, der Einsatz und die Verwaltung von Informationssystemen kann gesetzlichen, behördlichen und vertraglichen Sicherheitsanforderungen unterworfen sein.

Ratschläge zu spezifischen Rechtsvorschriften sollten von den Rechtsberatern der Organisation oder entsprechend qualifizierten Rechtsanwälten eingeholt werden.

Rechtsvorschriften sind von Land zu Land und für Informationen, die in einem Land erstellt wurden und in ein anderes Land übertragen werden (also ein grenzüberschreitender Datenfluss), unterschiedlich.

#### **12.1.1 Identifikation anwendbarer Gesetze**

Alle relevanten gesetzlichen, behördlichen und vertraglichen Anforderungen sollten für jedes Informationssystem ausdrücklich definiert und dokumentiert werden. Die spezifischen Maßnahmen und Verantwortungen einzelner Personen für die Erfüllung dieser Anforderungen sollten ähnlich definiert und dokumentiert werden.

#### **12.1.2 Rechte zum Schutz des geistigen Eigentums**

##### **12.1.2.1 Urheberrecht**

Es sollten entsprechende Verfahren implementiert werden, um zu gewährleisten, dass rechtliche Beschränkungen über den Gebrauch von Material, für das Rechte zum Schutz des geistigen Eigentums bestehen könnten, wie z.B. Urheberrechte, Entwurfsrechte, Warenzeichen, eingehalten werden. Urheberrechtsverletzungen können zu gerichtlichen Schritten führen, die eventuell Strafverfahren nach sich ziehen.

Gesetzliche, behördliche und vertragliche Anforderungen können das Kopieren von proprietärem Material einschränken. Insbesondere können sie verlangen, dass nur Material benutzt werden darf, das von der Organisation entwickelt wurde oder für das die Organisation eine Lizenz hat oder das der Organisation durch den Entwickler zur Verfügung gestellt wurde.

### 12.1.2.2 Software-Urheberrecht

Proprietäre Softwareprodukte werden gewöhnlich mit einem Lizenzvertrag geliefert, der die Benutzung der Produkte auf bestimmte Rechner und das Kopieren ausschließlich auf die Herstellung von Sicherheitskopien einschränken kann. Folgende Maßnahmen sollten in Erwägung gezogen werden:

- a) Veröffentlichung einer Politik zur Einhaltung des Software-Urheberrechts, die den gesetzlichen Gebrauch von Software und Informationsprodukten definiert;
- b) Herausgabe von Normen für Verfahren zur Akquisition von Softwareprodukten;
- c) Aufrechterhaltung des Bewusstseins über Politiken bezüglich des Software-Urheberrechts und der Software-Akquisition und Ausgabe einer Absichtserklärung, Disziplinarverfahren gegen Mitarbeiter einzuleiten, die gegen diese Politiken verstoßen;
- d) Aufrechterhaltung geeigneter Register der Werte;
- e) Aufheben von Belegen und Beweisen für den Besitz von Lizenzen, Originaldisketten, Handbücher usw.;
- f) Implementierung von Maßnahmen zur Sicherstellung, dass die maximal erlaubte Anzahl von Benutzern nicht überschritten wird;
- g) Durchführung von Prüfungen zur Sicherstellung, dass nur genehmigte Software und lizenzierte Produkte installiert sind;
- h) Bereitstellung einer Politik zur Erhaltung entsprechender Lizenzbedingungen;
- i) Bereitstellung einer Politik zur Entsorgung oder zum Transfer von Software an andere;
- j) Einsatz entsprechender Audittools;
- k) Einhaltung der Bedingungen für Software und Informationen, die über öffentliche Netze empfangen wurden (siehe auch 8.7.6).

### 12.1.3 Schutzmaßnahmen für organisationseigene Aufzeichnungen

Wichtige Aufzeichnungen einer Organisation sollten vor Verlust, Zerstörung und Fälschung geschützt werden. Einige Aufzeichnungen können eine sichere Aufbewahrung verlangen, um sowohl gesetzliche oder behördliche Anforderungen zu erfüllen als auch wesentliche Geschäftstätigkeiten zu unterstützen. Beispiele sind Aufzeichnungen, die als Beweis dafür erforderlich sind, dass eine Organisation im Einklang mit gesetzlichen oder behördlichen Vorschriften arbeitet, oder um eine adäquate Verteidigung bei potentiellen zivil- oder strafrechtlichen Verfahren sicherzustellen, oder die dazu dienen, den finanziellen Status einer Organisation gegenüber Aktionären, Partnern oder Auditoren zu bestätigen. Die Aufbewahrungsdauer und der Dateninhalt der Information kann von Gesetzen oder Regelungen des Landes festgelegt sein.

Aufzeichnungen sollten in Kategorien nach Aufzeichnungstypen aufbewahrt werden, z.B. Buchhaltungsaufzeichnungen, Datenbankaufzeichnungen, Transaktionsprotokolle, Auditprotokolle und betriebliche Verfahren, wobei für jeden Aufzeichnungstyp genaue Angaben zu Aufbewahrungsdauer und Speichermedientyp festzuhalten sind, z.B. Papier, Mikrofiche, magnetisch, optisch. Alle zugehörigen kryptographischen Schlüssel in Verbindung mit verschlüsselten Archiven oder digitalen Signaturen (siehe 10.3.2 und 10.3.3) sollten sicher aufbewahrt und berechtigten Personen bei Bedarf zur Verfügung gestellt werden.

Die Möglichkeit des Unbrauchbar-Werdens von Datenträgern, die zum Speichern von Aufzeichnungen benutzt werden, sollte in Erwägung gezogen werden. Verfahren zur Speicherung und Behandlung sollten in Übereinstimmung mit den Empfehlungen des Herstellers implementiert werden.

Sofern elektronische Speichermedien gewählt werden, sollten Verfahren zur Sicherstellung implementiert werden, dass während der Aufbewahrungsdauer auf Daten (sowohl in bezug auf Datenträger als auch auf die Lesbarkeit von Formaten) zugegriffen werden kann, um vor einem Verlust durch zukünftige Änderungen der Technologie zu schützen.

Datenspeicherungssysteme sollten so gewählt werden, dass benötigte Daten in einer Weise zurückerhalten werden können, die von einem Gericht akzeptiert wird, z.B. dass alle benötigten Aufzeichnungen innerhalb eines annehmbaren Zeitrahmens und in einem akzeptablen Format abgerufen werden können.

Das System der Speicherung und Behandlung sollte eine klare Identifikation von Aufzeichnungen und ihrer gesetzlichen oder behördlichen Aufbewahrungsdauer sicherstellen. Es sollte eine entsprechende Zerstörung der Aufzeichnungen nach diesem Zeitraum erlauben, wenn sie nicht von der Organisation benötigt werden.

Um diesen Verpflichtungen nachzukommen, sollten innerhalb einer Organisation folgende Schritte unternommen werden:

- a) Es sollten Richtlinien für die Aufbewahrung, Speicherung, Behandlung und Entsorgung von Aufzeichnungen und Informationen erstellt werden.
- b) Es sollte ein Zeitplan für die Aufbewahrung aufgestellt werden, der wesentliche Aufzeichnungstypen sowie die Aufbewahrungsdauer festlegt.
- c) Es sollte ein Inventar der Quellen von Schlüsselinformationen angelegt werden.
- d) Es sollten entsprechende Maßnahmen implementiert werden, um wesentliche Aufzeichnungen und Informationen vor Verlust, Zerstörung und Fälschung zu schützen.

#### **12.1.4 Datenschutz und Geheimhaltung persönlicher Informationen**

Viele Länder haben Gesetze für Maßnahmen bei der Verarbeitung und Übertragung persönlicher Daten (im allgemeinen Informationen zu lebenden Personen, die aufgrund dieser Informationen identifiziert werden können) eingeführt. Derartige Maßnahmen können denjenigen Pflichten auferlegen, die persönliche Daten sammeln, verarbeiten und verteilen, und die Möglichkeit, diese Daten in andere Länder zu übertragen, beschränken.

Die Einhaltung der Datenschutzgesetze erfordert eine entsprechende Managementstruktur und -kontrolle. Oft geschieht dies am besten durch die Ernennung eines Datenschutzbeauftragten, der Manager, Benutzer und Diensteanbieter über ihre einzelnen Verantwortlichkeiten und über die spezifischen Verfahren, nach denen gehandelt werden sollte, berät. Es sollte deshalb Aufgabe der für die Daten zuständigen Person sein, den Datenschutzbeauftragten über Vorschläge zur Speicherung von persönlichen Informationen in einer strukturierten Datei zu informieren, und für die Kenntnis der gesetzlich festgelegten Datenschutzprinzipien zu sorgen.

### **12.1.5 Vorbeugung gegen den Mißbrauch von Geräten zur Informationsverarbeitung**

Die Geräte zur Informationsverarbeitung in einer Organisation stehen Geschäftszwecken zur Verfügung. Ihre Benutzung sollte vom Management genehmigt werden. Jede Benutzung dieser Geräte für geschäftsfremde oder unerlaubte Zwecke ohne Zustimmung des Managements sollte als Missbrauch der Geräte betrachtet werden. Falls eine derartige Tätigkeit durch Überwachung oder andere Mittel festgestellt wird, sollte der zuständige Manager davon unterrichtet werden, um ein entsprechendes Disziplinarverfahren einzuleiten.

Die Rechtmäßigkeit einer Überwachung der Benutzung ist von Land zu Land unterschiedlich. Es kann erforderlich sein, Mitarbeiter über eine derartige Überwachung zu informieren oder ihr Einverständnis einzuholen. Vor der Implementierung von Überwachungsverfahren sollte rechtlicher Rat eingeholt werden.

Zahlreiche Länder haben Gesetze zum Schutz vor Rechnermissbrauch eingeführt oder sind dabei, sie einzuführen. Die Benutzung eines Rechners zu unerlaubten Zwecken kann als Straftat gelten. Es ist deshalb überaus wichtig, dass alle Benutzer die exakte Reichweite ihres erlaubten Zugriffs kennen. Dieses kann zum Beispiel durch eine schriftliche Genehmigung für Benutzer erreicht werden, von der eine Durchschrift vom Benutzer unterschrieben und diese sicher von der Organisation aufbewahrt werden sollte. Mitarbeiter einer Organisation und Benutzer von Fremdunternehmen sollten daraufhingewiesen werden, dass außer dem genehmigten Zugriff kein anderer Zugriff erlaubt ist.

Bei der Anmeldung sollte eine Warnmeldung auf dem Bildschirm erscheinen, die besagt, dass das System, auf das zugegriffen wird, privat ist, und dass ein unberechtigter Zugriff nicht erlaubt ist. Der Benutzer muss die Meldung auf dem Bildschirm entsprechend bestätigen und auf sie reagieren, um mit dem Anmeldeprozess fortfahren zu können.

### **12.1.6 Regelung kryptographischer Maßnahmen**

Einige Länder haben Vereinbarungen, Gesetze, Regelungen oder andere Instrumente implementiert, um den Zugriff auf oder die Verwendung von kryptographischen Maßnahmen zu kontrollieren. Derartige Maßnahmen können folgende Elemente beinhalten:

- a) Ein- und/oder Ausfuhr von Computer-Hardware und -Software zur Ausführung kryptographischer Funktionen;
- b) Ein- und/oder Ausfuhr von Computer-Hardware und -Software, zu der kryptographische Funktionen hinzugefügt werden sollen;
- c) Vorgeschriebene oder diskrete Zugriffsmethoden von den Ländern auf Informationen, die über Hardware oder Software verschlüsselt sind, um für eine Vertraulichkeit des Inhalts zu sorgen.

Zur Sicherstellung, dass die Gesetze des jeweiligen Landes eingehalten werden, sollte rechtlicher Rat eingeholt werden. Vor der Verlagerung verschlüsselter Informationen oder kryptographischer Maßnahmen in ein anderes Land sollte ebenfalls rechtlicher Rat eingeholt werden.

## 12.1.7 Sammeln von Beweisen

### 12.1.7.1 Regeln für Beweise

Zur Unterstützung eines Verfahrens gegen eine Person oder Organisation werden adäquate Beweise benötigt. Sofern es sich dabei um ein internes Disziplinarverfahren handelt, werden die benötigten Beweise durch interne Verfahren beschrieben.

Sofern es sich um ein gerichtliches Verfahren, entweder zivil- oder strafrechtlich, handelt, sollten die vorgelegten Beweise mit den Regeln für Beweise übereinstimmen, die im relevanten Gesetz oder in den Regeln des spezifischen Gerichts niedergelegt sind, vor dem der Fall verhandelt wird. Im allgemeinen decken diese Regeln folgende Punkte ab:

- a) Zulässigkeit von Beweisen: ob die Beweise vor Gericht verwendet werden können;
- b) Gewicht von Beweisen: die Qualität und Vollständigkeit der Beweise;
- c) Adäquate Beweise, dass Maßnahmen (also Prozeßkontrollbeweise) während des Zeitraums, in dem die zu sammelnden Beweise vom System gespeichert und verarbeitet wurden, richtig und konsistent funktioniert haben.

### 12.1.7.2 Zulässigkeit von Beweisen

Damit Beweise zulässig sind, sollten Organisationen sicherstellen, dass ihre Informationssysteme im Einklang mit allen veröffentlichten Normen oder Leitfäden für die Erstellung zulässiger Beweise stehen.

### 12.1.7.3 Qualität und Vollständigkeit von Beweisen

Für qualitativ hochwertige und vollständige Beweise wird eine starke Beweisführung benötigt. Im allgemeinen kann eine derart starke Beweisführung unter den folgenden Bedingungen hergestellt werden.

- a) Für Papierdokumente: Das Original wird sicher verwahrt und es wird aufgezeichnet, wer es gefunden hat, wo es gefunden wurde, wann es gefunden wurde und wer Zeuge bei der Entdeckung war. Bei Untersuchungen sollte sichergestellt werden, dass die Originale nicht verfälscht werden.
- b) Für Informationen auf Computemedien: Zur Sicherstellung, dass Informationen verfügbar sind, sollten Kopien jeglicher mobilen Datenträger, Informationen auf Festplatten oder im Speicher erstellt werden. Das Protokoll über alle Tätigkeiten während des Kopierprozesses sollte aufbewahrt und der Prozess von einem Zeugen beobachtet werden. Eine Kopie des Datenträgers und des Protokolls sollte sicher verwahrt werden.

Wenn ein Vorfall zuerst bemerkt wird, ist es unter Umständen nicht offensichtlich, dass er ein mögliches Gerichtsverfahren nach sich ziehen wird. Deshalb besteht die Gefahr, dass notwendige Beweise versehentlich zerstört werden, bevor die Ernsthaftigkeit des Vorfalls erkannt wird. Es ist ratsam, frühzeitig einen Anwalt oder die Polizei einzubeziehen, wenn gerichtliche Schritte erwogen werden und Rat einzuholen, welche Beweise erforderlich sind.

## 12.2 Überprüfungen der Sicherheitspolitik und der Einhaltung technischer Normen

Ziel: Sicherstellung der Erfüllung organisationseigener Sicherheitspolitiken und Normen durch Systeme.

Die Sicherheit von Informationssystemen sollte regelmäßig überprüft werden.

Derartige Überprüfungen sollten gegen die entsprechenden Sicherheitspolitiken vorgenommen werden und die technischen Plattformen und Informationssysteme sollten auf ihre Einhaltung von Normen der Sicherheitsimplementierung hin einem Audit unterzogen werden.

### 12.2.1 Einhaltung der Sicherheitspolitik

Manager sollten sicherstellen, dass alle Sicherheitsverfahren in ihrem Verantwortungsbereich korrekt ausgeführt werden. Zusätzlich sollte eine regelmäßige Überprüfung aller Bereiche innerhalb der Organisation in Betracht gezogen werden, um die Einhaltung der Sicherheitspolitiken und -normen zu gewährleisten. Diese Prüfung sollte sich auf folgende Bereiche erstrecken:

- a) Informationssysteme;
- b) Systemanbieter;
- c) zuständige Personen für Informationen und Informationswerte;
- d) Benutzer;
- e) Management.

Für Informationssysteme zuständige Personen (siehe 5.1) sollten regelmäßige Überprüfungen, ob ihre Systeme die entsprechenden Sicherheitspolitiken, Normen und andere Sicherheitsanforderungen erfüllen, unterstützen. Die Überwachung der Systembenutzung im Betrieb wird unter 9.7 behandelt.

### 12.2.2 Prüfung der Einhaltung technischer Normen

Informationssysteme sollten regelmäßig auf die Einhaltung der Normen für die Sicherheitsimplementierung hin überprüft werden. Die Prüfung der Einhaltung technischer Normen schließt die Überprüfung laufender Systeme mit ein, damit sichergestellt wird, dass Hardware- und Software-Maßnahmen korrekt implementiert wurden. Diese Art der Prüfung der Einhaltung von Normen erfordert eine fachmännische technische Hilfe. Sie sollte manuell (bei Bedarf mit Hilfe entsprechender Software-Tools) durch einen erfahrenen Systemingenieur vorgenommen werden, oder sie kann durch ein automatisiertes Softwarepaket vollzogen werden, das einen Bericht für die nachfolgende Interpretation durch eine technische Fachkraft generiert.

Die Prüfung der Einhaltung von Normen beinhaltet beispielsweise auch Penetrationstests, die von unabhängigen Experten durchgeführt werden können, mit denen speziell für diesen Zweck ein Vertrag abgeschlossen wurde. Dies kann nützlich sein, um Schwachstellen im System zu erkennen, und um die Effektivität der Maßnahmen zur Verhinderung eines unberechtigten Zugriffs aufgrund dieser Schwachstellen zu prüfen. Vorsicht ist angebracht,

wenn ein erfolgreicher Penetrationstest zu einer Kompromittierung der Sicherheit des System führen könnte und unbeabsichtigt andere Schwachstellen ausnutzt.

Technische Prüfungen der Einhaltung von Normen sollten nur durch kompetente, berechtigte Personen oder unter deren Aufsicht durchgeführt werden.

### **12.3 Überlegungen zum Systemaudit**

Ziel: Maximierung der Effektivität und Minimierung der Störungen beim Systemauditprozess.

Es sollten Maßnahmen zur Sicherung der laufenden Systeme und Audittools während Systemaudits existieren.

Ein Schutz ist ebenfalls erforderlich, um die Integrität von Audittools zu sichern und ihren Missbrauch zu verhindern.

#### **12.3.1 Maßnahmen für Systemaudits**

Auditanforderungen und -aktivitäten, die Prüfungen an laufenden Systemen betreffen, sollten sorgfältig geplant und vereinbart werden, um das Risiko von Störungen der Geschäftsprozesse zu vermindern.

Folgende Punkte sollten beachtet werden:

- a) Auditanforderungen sollten mit dem entsprechenden Management vereinbart werden.
- b) Der Anwendungsbereich der Prüfungen sollte vereinbart und kontrolliert werden.
- c) Die Prüfungen sollten auf nur lesenden Zugriff für Software und Daten begrenzt werden.
- d) Ein anderer Zugriff als nur lesender sollte nur für isolierte Kopien von Systemdateien erlaubt werden, die nach Beendigung des Audits gelöscht werden sollten.
- e) IT-Ressourcen für die Ausführung der Prüfungen sollten ausdrücklich identifiziert und verfügbar gemacht werden.
- f) Anforderungen für spezielle oder zusätzliche Verarbeitungen sollten identifiziert und vereinbart werden.
- g) Jeder Zugriff sollte überwacht und protokolliert werden, um ein Referenzprotokoll anzufertigen.
- h) Sämtliche Verfahren, Anforderungen und Zuständigkeiten sollten dokumentiert werden.

#### **12.3.2 Schutz der Systemaudittools**

Der Zugriff auf Systemaudittools, d.h., Software oder Dateien, sollte geschützt werden, um einen möglichen Missbrauch oder eine Kompromittierung zu vermeiden. Solche Tools sollten von der Entwicklung und von laufenden Systemen getrennt werden und nicht in Bandbibliotheken oder Benutzerbereichen gehalten werden, es sei denn, sie verfügen über ein ausreichendes Maß an zusätzlichem Schutz.

**Anhang** (informativ) Änderungen bei der internen Nummerierung

Tabelle A. 1 setzt die entsprechenden Abschnittsnummern der ersten Ausgabe dieses Teils der B S 7799 und dieser Ausgabe in Beziehung zueinander.

**Tabelle A. 1 — Beziehung zwischen internen Nummerierungen in verschiedenen Ausgaben dieses Teils der BS 7799**

Abschnittsnummer der Ausgabe 1995	Abschnittsnummer der Ausgabe 1999
Einleitung	Einleitung
0.1 Anwendungsbereich	1 Anwendungsbereich
0.3 Definitionen	2 Begriffe und Definitionen
1 Sicherheitsvorschriften	3 Sicherheitspolitik
1.1 Vorschriften zur Informationssicherheit	3. 1 Informationssicherheitspolitik
2 Sicherheitsorganisation	4 Organisation der Sicherheit
2.1 Infrastruktur der Informationssicherheit	4.1 Infrastruktur der Informationssicherheit
2.2 Sicherheit vor dem Zugang von Fremdunternehmen	4.2 Sicherheit beim Zugang durch Fremdunternehmen
	4.3 Outsourcing
3 Klassifizierung und Überwachung der Anlagen und Bestände	5 Einstufung und Kontrolle der Werte
3.1 Verantwortlichkeit für Anlagen und Bestände	5.1 Zurechenbarkeit für Werte
3.2 Klassifizierung der Information	5.2 Einstufung von Informationen
4 Sicherheit des Personals	6 Personelle Sicherheit
4.1 Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen	6.1 Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen
4.2 Benutzerschulung	6.2 Benutzerschulung
4.3 Reaktion auf Vorfälle	6.3 Verhalten bei Sicherheitsvorfällen und Störungen
5 Physische und umgebungsbezogene Sicherheit	7 Physische und umgebungsbezogene Sicherheit
5.1 Sicherheitszonen	7.1 Sicherheitszonen
5.2 Sicherheit der Geräte	7.2 Sicherheit der Geräte
	7.3 Allgemeine Maßnahmen
6 Rechner- und Netzverwaltung	8 Management der Kommunikation und des Betriebs
6.1 Betriebsverfahren und -Verantwortlichkeiten	8.1 Betriebsverfahren und -Verantwortlichkeiten
6.2 Systemplanung und -übernahme	8.2 Systemplanung und -abnahme
6.3 Schutz vor bösartiger Software	8.3 Schutz vor bösartiger Software
6.4 Haushaltsorganisation	8.4 Haushaltsorganisation
6.5 Netzverwaltung	8.5 Netzwerkmanagement
6.6 Umgang mit Datenträgern und Sicherheit	8.6 Umgang mit und Sicherheit von Datenträgern

6.7 Daten- und Softwareaustausch	8.7 Austausch von Informationen und Software
7 Systemzugriffskontrolle	9 Zugangskontrolle
7.1 Geschäftsanforderung für die Zugriffskontrolle	9.1 Geschäftsanforderung an die Zugangskontrolle
7.2 Verwaltung des Benutzerzugriffs	9.2 Verwaltung der Zugriffsrechte, der Benutzer
7.3 Verantwortung der Benutzer	9.3 Verantwortung der Benutzer
7.4 Netzzugriffskontrolle	9.4 Netzzugriffskontrolle
7.5 Rechnerzugriffskontrolle	9.5 Kontrolle des Betriebssystemzugriffs
7.6 Anwendungszugriffskontrolle	9.6 Zugriffskontrolle für Anwendungen

**Tabelle A. 1 - Beziehung zwischen internen Numerierungen in verschiedenen Ausgaben dieses Teils der BS 7799 (Forts.)**

7.7 Überwachung von Systemzugriff und der Systembenutzung	9.7 Überwachung des Systemzugriffs und der Systembenutzung
	9.8 Mobile Computing und Telearbeit
8 Systementwicklung und -Wartung	10 Systementwicklung und -Wartung
8.1 Sicherheitsanforderungen an Systeme	10.1 Sicherheitsanforderungen an Systeme
8.2 Sicherheit in Anwendungssystemen	10.2 Sicherheit in Anwendungssystemen
	10.3 Kryptographische Maßnahmen
8.3 Sicherheit von Anwendungssystemdateien	10.4 Sicherheit von Systemdateien
8.4 Sicherheit in Entwicklungs- und Supportumgebungen	10.5 Sicherheit bei Entwicklungs- und Supportprozessen
9 Geschäftskontinuitätsplanung	11 Management des kontinuierlichen Geschäftsbetriebs
9.1 Aspekte der Geschäftskontinuitätsplanung	11.1 Aspekte zur Aufrechterhaltung des Geschäftsbetriebs
10 Erfüllung der Verpflichtungen	12 Einhaltung der Verpflichtungen
10.1 Erfüllung gesetzlicher Verpflichtungen	12.1 Einhaltung gesetzlicher Verpflichtungen
10.2 Sicherheitsprüfungen von IT-Systemen	12.2 Überprüfungen der Sicherheitspolitik und der Einhaltung technischer Normen
10.3 Überlegungen zur Systemrevision	12.3 Überlegungen zum Systemaudit

## Stichwortverzeichnis

<b>Abnahme, System</b>	8.2.2
<b>Allgemeine physische Maßnahmen</b>	7.3
<b>Analyse Ihrer Sicherheitsrisiken,</b>	Einleitung
<b>Analyse von Risiken</b>	2.2
<b>Andere Formen des Informationsaustausches</b>	8.7.7
<b>Änderungskontrolle</b>	
—, betriebliche	8.1.2
—, Verfahren	10.5.1
<b>Anforderungen an Sicherheit,</b>	Einleitung
<b>Anmeldeverfahren, Terminal</b>	9.5.2
<b>Anstellungsbedingungen</b>	6.1.4
<b>Anwendbarkeit von Maßnahmen,</b>	Einleitung
<b>Anwendungsbereich</b>	1
<b>Anwendungssysteme, Sicherheit</b>	10.2
<b>Anwendungszugriffskontrolle</b>	9.6
<b>Arbeiten in Sicherheitsgrenzen</b>	7.1.4
<b>Arbeiten von zu Hause</b>	
—, Sicherheit der Telearbeit	9.8.2
—, Sicherheit von Geräten	7.2.5
<b>Arbeitsverantwortlichkeiten, Sicherheit</b>	6.1.1
<b>Audit</b>	
—Protokolle	9.7.1
—tools, Schutz	12.3.2
—Überlegungen	12.3
<b>Aufräumen des Schreibtischs und Löschen des Bildschirms, Politik</b>	7.3.1
<b>Aufrechterhaltung des Geschäftsbetriebs</b>	11
—, Management	11
—, Managementprozeß	11.1
—, Rahmen	11.1.4
—, Testen, Gewährleistung und erneute Analyse von Plänen	11.1.5
— und Auswirkungsanalyse	11.1.2
—, Verfassen und Implementieren von Plänen	11.1.3
<b>Ausbildung und Schulung in der Informationssicherheit</b>	6.2.1
<b>Ausgabedaten, Validierung</b>	10.2.4
<b>Austausch</b>	
—, Informationen und Software	8.7
—, Informationen und Software, Vereinbarungen	8.7.1
—, Informationen, andere Formen	8.7.7
<b>Authentisierung</b>	
—, Benutzer-	9.4.3
—, Knoten-	9.4.4
—, Nachrichten-	10.2.3
<b>Automatische Terminalidentifikation</b>	9.5.1
<b>Back-up von Informationen</b>	8.4.1
<b>Bedienerprotokolle</b>	8.4.2
<b>Bedingungen für Anstellungen</b>	6.1.4
<b>Begrenzung der Verbindungsdauer</b>	9.5.8
<b>Benutzer</b>	
—Anmeldung	9.2.1
—Authentisierung	9.5.3
—Identifikation	9.5.3
—Kennungen	9.2.1
—Passwortverwaltung	9.2.3
—Rechte, Überprüfung	9.2.4
—Schulung	6.2
—Verantwortung	9.3
—Verwaltung	9.2
—Zugriff	
—, Rechte, Überprüfung	9.2.4
—, —, Verwaltung	9.2
<b>Berechtigungsprozeß</b>	4.1.4
<b>Beschränkungen für Änderungen an Softwarepaketen</b>	10.5.3

## BS 7799-1:1999

<b>Betriebliche Änderungskontrolle</b>	<b>8.1.2</b>
<b>Betriebs-</b>	
—Software, Kontrolle	10.4.1
—systemzugriffskontrolle	9.5
—verfahren	8.1.1
—verfahren und -Verantwortlichkeiten	8.1
<b>Betriebs- und Kommunikationsmanagements</b>	
<b>Beweise, Sammeln</b>	<b>12.1.7</b>
<b>Bewertung und Überprüfung der Sicherheitspolitik</b>	<b>3.1.2</b>
<b>Bösartige Software</b>	
—, Maßnahmen	8.3.1
—, Schutz	8.3
<b>Bürosysteme, elektronische</b>	<b>8.7.5</b>
<b>Datenträger</b>	
—, Beseitigung	8.6.2
—, mobile	8.6.1
—, Transit	8.7.2
—, Umgang und Sicherheit	8.6
<b>Definition der Sicherheitsanforderungen, Einleitung</b>	
<b>Digitale Signaturen</b>	<b>10.3.3</b>
<b>Disziplinarprozeß</b>	<b>6.3.5</b>
<b>Dokumentation, Sicherheit von System-</b>	<b>8.6.4</b>
<b>Dokumentierte Betriebsverfahren</b>	<b>8.1.1</b>
<b>E-Commerce</b>	<b>8.7.3</b>
<b>E-Mail</b>	<b>8.7.4</b>
<b>Eingabedaten, Validierung</b>	
<b>Eingeschränkter Pfad</b>	<b>9.4.2</b>
<b>Einhaltung</b>	
—, gesetzlicher Verpflichtungen	12.1
—, Sicherheitspolitik	12.2.1
<b>Einstufung</b>	
—, Informationen	5.2
—, Richtlinien	5.2.1
—, Werte	5
<b>Elektronische Bürosysteme</b>	<b>8.7.5</b>
<b>Entfernung von Eigentum</b>	<b>7.3.2</b>
<b>Entsorgung</b>	
—, Datenträger	7.6.2
—, Geräte	7.2.6
<b>Entwicklung</b>	
—, Entwicklungs- und Betriebsanlagen, Trennung	8.1.5
—, Entwicklungs- und Supportumgebung, Sicherheit	10.5
— und Wartung von Systemen	10
<b>Entwicklung Ihrer eigenen Richtlinien, Einleitung</b>	
<b>Externe Verwaltung von Geräten</b>	<b>8.1.6</b>
<b>Fachliche Informationssicherheitsberatung</b>	<b>4.1.5</b>
<b>Fehler, Protokollieren</b>	<b>8.4.3</b>
<b>Formen des Informationsaustausches, andere</b>	<b>8.7.7</b>
<b>Fremdunternehmen</b>	
—, Identifikation der Risiken	4.2.1
—, Sicherheitsanforderungen in Verträgen	4.2.2
—, Zugang	4.2
<b>Funktionsstörungen, Meldung</b>	<b>6.3.3</b>
<b>Gefahren, Schutz der Geräte</b>	<b>7.2.1</b>
<b>Geräte</b>	
—, außerhalb der Geschäftsräume benutzte	7.2.5
—, Positionierung und Schutz	7.2.1
—, Sicherheit	7.2
—, Sicherheit der Geschäftsräume und -,	7.1.3
—, unbeaufsichtigte	9.3.2
—, <b>Wartung</b>	<b>7.2.4</b>
<b>Geschäftsanforderungen an die Zugangskontrolle</b>	<b>9.1</b>
<b>Geschäftsräume und Geräte, Sicherung</b>	<b>7.1.7</b>
<b>Haushaltsorganisation</b>	<b>8.4</b>

<b>Herunterladen von Informationen und Software</b>	8.1.3,8.7.4,10.2.2
<b>Identifikation der anwendbaren Gesetzgebung</b>	12.1.1
<b>Identifikation von Benutzern</b>	9.5.3
<b>Identifikation von Terminals</b>	9.5.1
<b>Informationen</b>	
—, andere Formen des Austausches	8.7.7
—, Back-ups.	4.1
—, Einstufung	5.2
—, Kennzeichnung und Behandlung	5.2.2
— und Software, Austausch	8.7
— und Vereinbarungen über den Austausch von Software	8.7.1
—, Verfahren zum Umgang	8.6.3
—, Zugriff, Beschränkungen	9.6.1
<b>Informationssicherheit</b>	2.1
—, Anforderungen,	<b>Einleitung</b>
—, Ausbildung und Schulung	6.2.1
—, Dokument zur Politik	3.1.1
—, Infrastruktur	4.1
—, Koordination	4.1.2
—,Politik	3.1
<b>Integrität</b>	2.1
<b>Interne Verarbeitung, Kontrolle</b>	10.2.2
<b>Inventar der Werte</b>	5.1.1
<b>Isolierung sensibler Systeme</b>	9.6.2
<b>Kapazitätsplanung</b>	8.2.1
<b>Kennzeichnung und Behandlung von Informationen</b>	5.2.2
<b>Kommunikations- und Betriebsmanagement</b>	8
<b>Knoten-Authentisierung</b>	9.4.4
<b>Kontrolle</b>	
—, Systembenutzung	9.7.2
—, Systemzugriff und Systembenutzung	9.7
<b>Kritische Erfolgsfaktoren, Einleitung Kryptographische Maßnahmen</b>	10.3
—, Politik für den Einsatz	10.3.1
—, Regelung	10.3.2
<b>Leitprinzipien, Einleitung Lernen aus Vorfällen</b>	6.3.4
<b>Liefer- und Ladebereiche</b>	7.1.5
<b>Management</b>	
—, Informationssicherheitsforum	4.1.1
—, Kommunikation und Betrieb	8
—, Netze	8.5
—, Risiko	2.3
<b>Maßnahmen</b>	
—, allgemeine physische	7.3
—, böartige Software	8.3.1
—, Kontrolle für interne Verarbeitung	10.2.2
—, Kontrolle von Software in laufenden Systemen	10.4.1
<b>Meldung</b>	
—, Sicherheitsschwachstellen	6.3.2
—, Sicherheitsvorfällen	6.3.1
—, Softwarefunktionsstörungen	6.3.3
<b>Mißbrauch von Geräten zur Informationsverarbeitung</b>	12.1.5
<b>Mobile Computing</b>	9.8.1
— und Telearbeit	9.8
<b>Nachrichtenauthentisierung</b>	10.2.3
<b>Netz</b>	
—, Kontrolle der Verbindung	9.4.7
—, Management	8.5
—, Routing-Kontrolle	9.4.8
—, Trennung	9.4.6
—, Zugriffskontrolle	9.4
<b>Nicht-Abstreitbarkeitservice</b>	10.3.4

## BS 7799-1:1999

<b>Öffentlich zugängliche Systeme</b>	8.7.6
<b>Organisation der Sicherheit</b>	4
<b>Organisationseigene Aufzeichnungen, Schutzmaßnahmen</b>	12.1.3
<b>Outsourcing</b>	4.3
—, Sicherheit in Verträgen	4.3.1
—, Softwareentwicklung außerhalb der Organisation	10.5.5
<b>Passwörter</b>	
—, Gebrauch	9.3.1
—, Verwaltung, Benutzer-	9.2.3
—, Verwaltungssystem	9.5.4
<b>Personelle Sicherheit</b>	6
<b>Persönliche Informationen, Geheimhaltung</b>	12.1.4
<b>Physische</b>	
— Sicherheitsgrenze	7.1.1
— und umgebungsbezogene Sicherheit	7
— Zutrittskontrollen	7.1.2
<b>Politik</b>	
—, Einsatz kryptographischer Maßnahmen	10.3.1
—, Sicherheit	3
—, Verwendung von Netzdiensten	9.4.1
—, Zugangskontrolle	9.1
<b>Positionierung von Geräten</b>	7.2.1
<b>Programmquellenbibliothek, Zugriffskontrolle</b>	10.4.3
<b>Protokolle, Bediener-</b>	8.4.2
<b>Protokollieren</b>	
—, Fehler	8.4.3
—, Vorfälle	9.7.1
<b>Rahmen für Pläne zur Aufrechterhaltung des Geschäftsbetriebs</b>	11.1.4
<b>Rechte zum Schutz des geistigen Eigentums</b>	12.1.2
<b>Reserveplanung</b>	11.1.3
<b>Risikoanalyse</b>	2.2
<b>Risikomanagement</b>	2.3
<b>Routing-Kontrolle</b>	9.4.8
<b>Sammeln von Beweisen</b>	12.1.7
<b>Schlüsselmanagement</b>	10.3.5
<b>Schulung</b>	6.2.1
<b>Schutz</b>	
—, bösartige Software	8.3
—, Geräte, vor Gefahren	7.2
—, Systemaudittools	12.3.2
—, Systemtestdaten	10.4.2
<b>Schutz des Ferndiagnoseports</b>	9.4.5
<b>Schutz des geistigen Eigentums, Rechte</b>	12.1.2
<b>Schutzmaßnahmen für organisationseigene Aufzeichnungen</b>	12.1.3
<b>Sensitive Systeme, Isolierung</b>	9.6.2
<b>Separate Liefer- und Ladebereiche</b>	7.1.5
<b>Sicherheit</b>	
—, Anforderungen an Systeme	10.1
—, Anforderungen in Outsourcing-Verträgen	4.3.1
—, Anforderungen in Verträgen mit Fremdunternehmen	4.2
—, Anforderungsanalyse	10.1.1
—, Anwendungssysteme	10.2
—, Ausbildung	6.2.1
—, Datenträger im Transit	8.7.2
—, elektronische Bürosysteme	8.7.5
—, E-Mail	8.7.4
—, E-Commerce	8.7.3
—, Einhaltung der Sicherheitspolitik	12.2.1
—, Entwicklungs- und Supportprozessen	10.5
—, Geschäftsräume und Geräte	7.1.3
—, Organisation	4
—, Schwachstellen, Meldung von	6.3.2
—, Sicherheitspolitik	3
—, Sicherheitsvorfälle	6.3,6.3.1
—, Systemdateien	10.4
—, Systemdokumentation	8.6.4

## BS 7799-1:1999

—, Überprüfungen der Geräte zur Informationsverarbeitung	12.2
—, Verkabelung	7.2.3
—, Zugang durch Fremdunternehmen	4.2
<b>Sicherheitsgrenzen</b>	7.1.1
<b>Sicherheitszonen</b>	7.1
—, Arbeiten	7.1.4
—, Entsorgung von Geräten	7.2.6
<b>Software</b>	
—, böartige, Schutz	6.3
—, Funktionsstörungen	6.3.3
—, Kontrolle in laufenden Systemen	10.4.1
—, Kopieren	12.1.2.2
—, Pakete, Beschränkungen für Änderungen	10.5.3
<b>Stellenbeschreibung und Bereitstellung von Ressourcen</b>	6.1
<b>Stromversorgung</b>	7.2.2
<b>Synchronisation der Uhren</b>	9.7.3
<b>System</b>	
—, Auditmaßnahmen	12.3.1
—, Auditüberlegungen	12.3
—, Dateien, Sicherheit	10.4
—, Dokumentation	8.6.4
—, Entwicklung und Wartung	10
—, Planung und Abnahme	8.2
—, sensitives, Isolierung	9.6.2
—, Testdaten, Schutz	10.4.2
<b>Technische</b>	
—, Normeinhaltungsprüfung	12.2.2
—, Überprüfung der Betriebssystemänderungen	10.5.2
<b>Telearbeit</b>	9.8.2
<b>Terminal</b>	
—, Anmeldeverfahren	9.5.2
—identifikation	9.5.1
—Timeout	9.5.7
<b>Test</b>	
—daten, Schutz,	10.4.2
— Testen, Aurrechterhaltung und erneute Analyse von Plänen zur Gewährleistung des kontinuierlichen Geschäftsbetrieb	
<b>11.1.5 Trennung</b>	
—, Entwicklungs- und Betriebsanlagen	8.1.5
—, Netze	9.4.6
—, Pflichten	8.1.4
<b>Trojanischer Code und verdeckte Kanäle</b>	10.5.4
<b>Überprüfung</b>	
—, Benutzerzugriffsrechte	9.2.4
—, Informationssicherheit	4.1.7
—, Mitarbeiter und Personalpolitik	6.1.2
— und Bewertung der Sicherheitspolitik	3.1.2
Uhrensynchronisation	9.7.3
<b>Umgebungsbezogene und physische Sicherheit</b>	7
<b>Unabhängige Überprüfung der Informationssicherheit</b>	4.1.7
<b>Unbeaufsichtigte Benutzergeräte</b>	9.3.2
<b>Urheberrecht</b>	
—, Rechte zum Schutz des geistigen Eigentums	12.1.2
—, Software	12.1.2.2
<b>Validierung</b>	
—, Ausgabedaten	10.2.3
—, Eingabedaten	10.2.1
<b>Verantwortlichkeiten</b>	
—, Benutzer	9.3
—, Sicherheit bei der Arbeit	6.1.1
<b>Verdeckte Kanäle und trojanischer Code</b>	10.5.4

## **BS 7799-1:1999**

<b>Verfahren im Notfall</b>	<b>11.13</b>
<b>Verfügbarkeit</b>	<b>2.1</b>
<b>Verhalten bei Vorfällen</b>	<b>6.3</b>
<b>Verhinderung des Mißbrauchs von Geräten zur Informationsverarbeitung</b>	<b>12.1.5</b>
<b>Verschlüsselung</b>	<b>10.3.2</b>
<b>Verträge</b>	
—, Sicherheit in Outsourcing- Verträgen	<b>4.3.1</b>
—, Sicherheit in Verträgen mit Fremdunternehmen	<b>4.2.2</b>
<b>Vertraulichkeit</b>	<b>2.1</b>
<b>Vertraulichkeitsvereinbarungen</b>	<b>6.1.3</b>
<b>Verwaltung</b>	
—, Benutzerzugriffsrechte	<b>9.2</b>
—, externe, Geräte	<b>8.1.6</b>
—, mobile Datenträger	<b>8.6.1</b>
—, Privilegien	<b>9.2.2</b>
<b>Virenkontrollen</b>	<b>8.3</b>
<b>Vorfälle</b>	
—, Lernen aus Vorfällen	<b>6.3.4</b>
—, Managementverfahren	<b>8.1.3</b>
—, Meldung von Vorfällen	<b>6.3.1</b>
—,Protokollieren	<b>9.7.1</b>
— und Funktionsstörungen, Meldung	<b>6.3</b>
<b>Werte, Einstufung und Kontrolle</b>	<b>5</b>
<b>Zertifizierung</b>	<b>10.3.5.2</b>
<b>Zugangskontrolle</b>	<b>9</b>
—, Betriebssystem	<b>9.5</b>
—, Geschäftsanforderungen	<b>9.1</b>
—,Politik	<b>9.1.1</b>
<b>Zugriffskontrolle</b>	
—, Anwendungen	<b>9.6</b>
—, Programmquellenbibliothek	<b>10.4.3</b>
<b>Zugriffsbeschränkung, auf Informationen</b>	<b>9.6.1</b>
<b>Zurechenbarkeit für Werte</b>	<b>5.1</b>
<b>Zusammenarbeit zwischen Organisationen</b>	<b>4.1.6</b>
<b>Zutrittskontrollen</b>	<b>7.1.2</b>
<b>Zuweisung der Zuständigkeiten für Informationssicherheit</b>	<b>4.1.3</b>
<b>Zwangsalarm</b>	<b>9.5.6</b>