

DIN ISO/IEC 27002

ICS 35.040

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden für das Informationssicherheits-Management
(ISO/IEC 27002:2005)**

Information technology –
Security techniques –
Code of practice for information security management (ISO/IEC 27002:2005)

Technologies de l'information –
Techniques de sécurité –
Code de bonne pratique pour la gestion de la sécurité de l'information
(ISO/CEI 27002:2005)

Gesamtumfang 138 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Inhalt

	Seite
Nationales Vorwort	6
Nationaler Anhang NA (informativ) Literaturhinweise.....	7
0 Einleitung.....	8
0.1 Was ist Informationssicherheit?	8
0.2 Warum ist Informationssicherheit notwendig?	8
0.3 Festlegung der Sicherheitsanforderungen	9
0.4 Einschätzung der Sicherheitsrisiken.....	9
0.5 Auswahl von Maßnahmen.....	9
0.6 Ausgangspunkt für Informationssicherheit.....	10
0.7 Entscheidende Erfolgsfaktoren.....	10
0.8 Entwicklung eigener Richtlinien	11
1 Anwendungsbereich	12
2 Begriffe	12
3 Aufbau dieser Norm	14
3.1 Abschnitte	14
3.2 Wesentliche Sicherheitskategorien	14
4 Risikoeinschätzung und -behandlung.....	15
4.1 Einschätzung der Sicherheitsrisiken.....	15
4.2 Umgang mit Sicherheitsrisiken.....	15
5 Sicherheitsleitlinie	17
5.1 Informationssicherheitsleitlinie.....	17
5.1.1 Leitlinie zur Informationssicherheit.....	17
5.1.2 Überprüfung der Informationssicherheitsleitlinie	18
6 Organisation der Informationssicherheit	19
6.1 Interne Organisation.....	19
6.1.1 Engagement des Managements für Informationssicherheit	19
6.1.2 Koordination der Informationssicherheit.....	20
6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit.....	20
6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen	21
6.1.5 Vertraulichkeitsvereinbarungen.....	21
6.1.6 Kontakt zu Behörden.....	22
6.1.7 Kontakt zu speziellen Interessengruppen.....	23
6.1.8 Unabhängige Überprüfung der Informationssicherheit.....	23
6.2 Externe.....	24
6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern.....	24
6.2.2 Adressieren von Sicherheit im Umgang mit Kunden.....	26
6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten	27
7 Management von organisationseigenen Werten.....	30
7.1 Verantwortung für organisationseigene Werte (Assets)	30
7.1.1 Inventar der organisationseigenen Werte (Assets).....	30
7.1.2 Eigentum von organisationseigenen Werten (Assets)	31
7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets).....	31
7.2 Klassifizierung von Informationen.....	32
7.2.1 Regelungen für die Klassifizierung.....	32
7.2.2 Kennzeichnung von und Umgang mit Informationen	33

8	Personalsicherheit	33
8.1	Vor der Anstellung	33
8.1.1	Aufgaben und Verantwortlichkeiten	34
8.1.2	Überprüfung	34
8.1.3	Arbeitsvertragsklauseln	35
8.2	Während der Anstellung	36
8.2.1	Verantwortung des Managements	36
8.2.2	Sensibilisierung, Ausbildung und Schulung für Informationssicherheit	37
8.2.3	Disziplinarverfahren	37
8.3	Beendigung oder Änderung der Anstellung	38
8.3.1	Verantwortlichkeiten bei der Beendigung	38
8.3.2	Rückgabe von organisationseigenen Werten	38
8.3.3	Zurücknahme von Zugangsrechten	39
9	Physische und umgebungsbezogene Sicherheit	39
9.1	Sicherheitsbereiche	39
9.1.1	Sicherheitszonen	40
9.1.2	Zutrittskontrolle	40
9.1.3	Sicherung von Büros, Räumen und Einrichtungen	41
9.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung	41
9.1.5	Arbeiten in Sicherheitszonen	42
9.1.6	Öffentlicher Zugang, Anlieferungs- und Ladezonen	42
9.2	Sicherheit von Betriebsmitteln	43
9.2.1	Platzierung und Schutz von Betriebsmitteln	43
9.2.2	Unterstützende Versorgungseinrichtungen	44
9.2.3	Sicherheit der Verkabelung	44
9.2.4	Instandhaltung von Gerätschaften	45
9.2.5	Sicherheit von außerhalb des Standorts befindlicher Ausrüstung	45
9.2.6	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	46
9.2.7	Entfernung von Eigentum	46
10	Betriebs- und Kommunikationsmanagement	47
10.1	Verfahren und Verantwortlichkeiten	47
10.1.1	Dokumentierte Betriebsprozesse	47
10.1.2	Änderungsverwaltung	48
10.1.3	Aufteilung von Verantwortlichkeiten	49
10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen	49
10.2	Management der Dienstleistungserbringung von Dritten	50
10.2.1	Erbringung von Dienstleistungen	50
10.2.2	Überwachung und Überprüfung der Dienstleistungen von Dritten	50
10.2.3	Management von Änderungen an Dienstleistungen von Dritten	51
10.3	Systemplanung und Abnahme	52
10.3.1	Kapazitätsplanung	52
10.3.2	Systemabnahme	52
10.4	Schutz vor Schadsoftware und mobilem Programmcode	53
10.4.1	Maßnahmen gegen Schadsoftware	53
10.4.2	Schutz vor mobiler Software (mobilen Agenten)	54
10.5	Backup	55
10.5.1	Backup von Informationen	55
10.6	Management der Netzsicherheit	56
10.6.1	Maßnahmen für Netze	56
10.6.2	Sicherheit von Netzdiensten	57
10.7	Handhabung von Speicher- und Aufzeichnungsmedien	58
10.7.1	Verwaltung von Wechselmedien	58
10.7.2	Entsorgung von Medien	58
10.7.3	Umgang mit Informationen	59
10.7.4	Sicherheit der Systemdokumentation	60
10.8	Austausch von Informationen	60

10.8.1	Leitlinien und Verfahren zum Austausch von Informationen	60
10.8.2	Vereinbarungen zum Austausch von Informationen	62
10.8.3	Transport physischer Medien.....	63
10.8.4	Elektronische Mitteilungen/Nachrichten (Messaging)	63
10.8.5	Geschäftsinformationssysteme	64
10.9	E-Commerce-Anwendungen.....	65
10.9.1	E-Commerce.....	65
10.9.2	Online-Transaktionen.....	66
10.9.3	Öffentlich verfügbare Informationen	67
10.10	Überwachung	67
10.10.1	Auditprotokolle	68
10.10.2	Überwachung der Systemnutzung.....	68
10.10.3	Schutz von Protokollinformationen	70
10.10.4	Administrator- und Betreiberprotokolle	70
10.10.5	Fehlerprotokolle.....	71
10.10.6	Zeitsynchronisation.....	71
11	Zugangskontrolle.....	72
11.1	Geschäftsanforderungen für Zugangskontrolle.....	72
11.1.1	Leitlinie zur Zugangskontrolle.....	72
11.2	Benutzerverwaltung	73
11.2.1	Benutzerregistrierung	73
11.2.2	Verwaltung von Sonderrechten.....	74
11.2.3	Verwaltung von Benutzerpasswörtern	75
11.2.4	Überprüfung von Benutzerberechtigungen	75
11.3	Benutzerverantwortung	76
11.3.1	Passwortverwendung.....	76
11.3.2	Unbeaufsichtigte Benutzerausstattung.....	77
11.3.3	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	77
11.4	Zugangskontrolle für Netze	78
11.4.1	Regelwerk zur Nutzung von Netzdiensten	78
11.4.2	Benutzerauthentisierung für externe Verbindungen	79
11.4.3	Geräteidentifikation in Netzen	80
11.4.4	Schutz der Diagnose- und Konfigurationsports.....	80
11.4.5	Trennung in Netzen	80
11.4.6	Kontrolle von Netzverbindungen	81
11.4.7	Routingkontrolle für Netze.....	82
11.5	Zugriffskontrolle auf Betriebssysteme.....	82
11.5.1	Verfahren für sichere Anmeldung.....	82
11.5.2	Benutzeridentifikation und Authentisierung.....	83
11.5.3	Systeme zur Verwaltung von Passwörtern	84
11.5.4	Verwendung von Systemwerkzeugen	85
11.5.5	Session Time-out.....	85
11.5.6	Begrenzung der Verbindungszeit	86
11.6	Zugangskontrolle zu Anwendungen und Information	86
11.6.1	Einschränkung von Informationszugriffen	86
11.6.2	Isolation sensibler Systeme	87
11.7	Mobile Computing und Telearbeit.....	87
11.7.1	Mobile Computing und Kommunikation.....	87
11.7.2	Telearbeit	88
12	Beschaffung, Entwicklung und Wartung von Informationssystemen	90
12.1	Sicherheitsanforderungen von Informationssystemen	90
12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen.....	90
12.2	Korrekte Verarbeitung in Anwendungen.....	91
12.2.1	Überprüfung von Eingabedaten	91
12.2.2	Kontrolle der internen Verarbeitung.....	92
12.2.3	Integrität von Nachrichten	93

12.2.4	Überprüfung von Ausgabedaten	93
12.3	Kryptographische Maßnahmen.....	93
12.3.1	Leitlinie zur Anwendung von Kryptographie.....	94
12.3.2	Verwaltung kryptographischer Schlüssel	95
12.4	Sicherheit von Systemdateien	96
12.4.1	Kontrolle von Software im Betrieb	96
12.4.2	Schutz von Test-Daten.....	97
12.4.3	Zugangskontrolle zu Quellcode.....	98
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen	99
12.5.1	Änderungskontrollverfahren.....	99
12.5.2	Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem	100
12.5.3	Einschränkung von Änderungen an Softwarepaketen.....	100
12.5.4	Ungewollte Preisgabe von Informationen.....	101
12.5.5	Ausgelagerte Softwareentwicklung.....	101
12.6	Umgang mit Schwachstellen.....	102
12.6.1	Kontrolle technischer Schwachstellen	102
13	Umgang mit Informationssicherheitsvorfällen.....	103
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen.....	103
13.1.1	Melden von Informationssicherheitsereignissen.....	104
13.1.2	Melden von Sicherheitsschwachstellen.....	105
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen.....	105
13.2.1	Verantwortlichkeiten und Verfahren.....	105
13.2.2	Lernen von Informationssicherheitsvorfällen	107
13.2.3	Sammeln von Beweisen	107
14	Sicherstellung des Geschäftsbetriebs (Business Continuity Management)	108
14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management).....	108
14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs	109
14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung	109
14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten.....	110
14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	111
14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs	112
15	Einhaltung von Vorgaben (Compliance).....	113
15.1	Einhaltung gesetzlicher Vorgaben	113
15.1.1	Identifikation der anwendbaren Gesetze	113
15.1.2	Rechte an geistigem Eigentum	113
15.1.3	Schutz von organisationseigenen Aufzeichnungen.....	114
15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen.....	115
15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen	116
15.1.6	Leitlinien zu kryptographischen Verfahren	117
15.2	Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben	117
15.2.1	Einhaltung von Sicherheitsleitlinien und -standards	117
15.2.2	Prüfung der Einhaltung technischer Vorgaben	118
15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen	118
15.3.1	Maßnahmen für Audits von Informationssystemen	119
15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme	119
	Literaturhinweise.....	120
	Stichwortverzeichnis.....	121

Nationales Vorwort

Die Internationale Norm ISO/IEC 27002:2005-06 wurde in deutscher Sprachfassung unverändert in das Deutsche Normenwerk übernommen. Fachlich zuständig ist für diese Deutsche Norm der Arbeitsausschuss NA 043-01-27 AA „IT-Sicherheitsverfahren“ des Normenausschusses Informationstechnik und Anwendungen (NIA) im DIN.

Die dieser Norm zugrunde liegende Internationale Norm ISO/IEC 27002 wurde von ISO/IEC JTC 1/SC 27 (International Organization for Standardization/International Electrotechnical Commission – Joint Technical Committee 1 „Information Technology“/Subcommittee 27 „Security techniques“) erarbeitet.

ISO/IEC 27002 ist aus dem Britischen Standard BS 7799-1 hervorgegangen. Grundsätzlich ist diese Norm dort anzuwenden, wo ein Schutzbedarf für Informationen besteht. Ziel des Dokuments ist es, Informationssicherheit als Gesamtaufgabe darzustellen, da es Leitlinien und allgemeine Grundsätze zum Management von IT-Sicherheit in einem Unternehmen (KP) enthält. In den Prozess der Informationssicherheit sind alle Bereiche der Organisation einzubeziehen, da alle an der Erhebung, Verarbeitung, Speicherung, Löschung von Informationen beteiligt sind. Der Anwendungsbereich ist somit ohne einen konkreten Bezug zu den Anforderungen in einer Organisation nicht abgrenzbar.

In ISO/IEC JTC 1/SC 27 wird zurzeit eine Internationale Normenreihe von Informationssicherheits-Managementsystemen (ISMS) entwickelt. Diese Normenreihe beinhaltet Internationale Normen zu den Themen — Anforderungen an ein Informationssicherheits-Managementsystem, Risikomanagement, Metriken und Maße, und eine Richtlinie zur Umsetzung. Diese Familie wird das Nummerierungsschema mit den Zahlen 27000 ff. annehmen.

Aufgrund der oben genannten Bestrebungen, alle ISMS-Standards, als ISO/IEC 27000er-Reihe zusammenzuführen, wurde ISO/IEC 17799:2005-06 (2. Ausgabe) in ISO/IEC 27002:2005-06 (1. Ausgabe) umbenannt. Demzufolge wird der Entwurf E DIN ISO/IEC 17799:2007-02 als Norm unter der Nummer DIN ISO/IEC 27002 veröffentlicht.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 9001	siehe DIN EN ISO 9001
ISO 14001	siehe DIN EN ISO 14001
ISO 19011	siehe DIN EN ISO 19011
ISO/IEC 27001	siehe DIN ISO/IEC 27001

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 14001, *Umweltmanagementsysteme — Anforderungen mit Anleitung zur Anwendung*

DIN EN ISO 19011, *Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen*

DIN ISO/IEC 27001, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005)*

Informationstechnik IT-Sicherheitsverfahren Leitfaden für das Informationssicherheits-Management

0 Einleitung

0.1 Was ist Informationssicherheit?

Informationen sind Werte, die genauso wie andere wichtige Geschäftswerte essentiell für den Geschäftsbetrieb von Organisationen sind und infolgedessen in geeigneter Weise geschützt werden müssen. In einer zunehmend vernetzten Geschäftswelt ist dies besonders wichtig. Als Ergebnis dieser zunehmenden Vernetzung sind Informationen heutzutage einer anwachsenden Zahl von Bedrohungen und Schwachstellen ausgesetzt (siehe auch OECD Guidelines for the Security of Information Systems and Networks).

Informationen können in vielen Formen vorliegen. Sie können auf Papier ausgedruckt oder geschrieben, elektronisch gespeichert, auf dem Postweg oder elektronisch übertragen, in Filmen gezeigt oder in Gesprächen weitergegeben werden. Unabhängig von der gewählten Form, dem Medium der Weitergabe oder Speicherung sollten Informationen immer angemessen geschützt werden.

Informationssicherheit ist der Schutz von Informationen vor einer Vielzahl von Bedrohungen, die Aufrechterhaltung des Geschäftsbetriebs sicherzustellen, Geschäftsrisiken zu minimieren und die Rendite und Geschäftschancen zu maximieren.

Informationssicherheit wird durch die Umsetzung geeigneter Maßnahmen erreicht, die Leitlinien, Prozesse, Verfahren, Organisationsstrukturen oder Software- und Hardwarefunktionen sein können. Diese Maßnahmen müssen eingeführt, umgesetzt, überwacht, überprüft und, falls nötig, verbessert werden, um sicherzustellen, dass die spezifischen Sicherheits- und Geschäftsziele der Organisation erfüllt werden. Dies sollte im Einklang mit anderen Geschäftsmanagementprozessen geschehen.

0.2 Warum ist Informationssicherheit notwendig?

Informationen und die sie unterstützenden Prozesse, Systeme und Netze sind wichtige Geschäftswerte. Definition, Erreichen, Pflege und Verbesserung von Informationssicherheit können wesentlich zur Erhaltung von Wettbewerbsfähigkeit, Liquidität, Rentabilität, Einhaltung gesetzlicher Vorschriften und Geschäftsansehen beitragen.

Organisationen und deren Informationssysteme und -netze sehen sich Sicherheitsbedrohungen unterschiedlichster Herkunft ausgesetzt, einschließlich Computerbetrug, Spionage, Sabotage, Vandalismus, und Naturkatastrophen wie Feuer oder Überschwemmung. Gefahrenquellen wie bösartiger Code, Hacker und Denial-of-Service-Attacken treten immer häufiger auf und werden dabei anspruchsvoller und raffinierter.

Informationssicherheit ist sowohl für den öffentlichen wie für den privaten Sektor wichtig, und auch, um kritische Infrastrukturen zu schützen. Für beide Sektoren stellt Informationssicherheit einen entscheidenden Faktor dar, der ermöglicht, dass beispielsweise E-Government oder E-Business eingesetzt wird, und relevante Risiken vermieden oder reduziert werden können. Die Verbindung von öffentlichen und privaten Netzen und die gemeinsame Nutzung von Informationsressourcen erhöhen die Schwierigkeit, die Zugangskontrolle zu gewährleisten. Der Trend hin zur verteilten Verarbeitung hat die Effektivität einer zentralen, fachlichen Kontrolle geschwächt.

Viele Informationssysteme wurden nicht entwickelt, um sicher zu sein. Die durch technische Mittel erreichbare Sicherheit ist begrenzt und sollte durch entsprechendes Management und entsprechende Verfahren unter-

stützt werden. Die Identifizierung der benötigten Maßnahmen erfordert sorgfältige Planung und Detailgenauigkeit. Die Mitwirkung aller Beschäftigten in einer Organisation ist eine Mindestvoraussetzung für Informationssicherheit. Außerdem kann auch die Mitwirkung von Anteilseignern, Zulieferern, Dritten, Kunden oder sonstigen externen Parteien erforderlich sein. Eine Fachberatung durch externe Organisationen kann ebenfalls erforderlich sein.

0.3 Festlegung der Sicherheitsanforderungen

Es ist äußerst wichtig, dass eine Organisation ihre Sicherheitsanforderungen identifiziert. Dabei gibt es drei wesentliche Quellen für Sicherheitsanforderungen.

1. Eine Quelle liefert die Risikoeinschätzung für die Organisation, wobei die allgemeinen Geschäftsstrategien und Ziele der Organisation berücksichtigt werden sollten. Durch eine Risikoeinschätzung werden Bedrohungen für vorhandene Werte identifiziert, Schwachstellen und Eintrittswahrscheinlichkeiten bewertet und die möglichen Auswirkungen abgeschätzt.
2. Die weitere Quelle sind Anforderungen, die sich aus Gesetzen, Politik, Regelungen und Verträgen ergeben und die von einer Organisation und ihren Handelspartnern, Vertragspartnern, und Dienstleistern erfüllt werden müssen, sowie die soziokulturelle Umgebung.
3. Eine weitere Quelle sind die spezifischen Prinzipien, Ziele und geschäftlichen Anforderungen an die Informationsverarbeitung, die eine Organisation entwickelt hat, um ihren Geschäftsbetrieb zu unterstützen.

0.4 Einschätzung der Sicherheitsrisiken

Sicherheitsanforderungen werden durch eine methodische Betrachtung von Sicherheitsrisiken ermittelt. Der Aufwand für Maßnahmen muss gegenüber dem wirtschaftlichen Schaden, der sich aus Sicherheitsproblemen ergeben kann, abgewogen werden.

Die Ergebnisse der Risikoeinschätzung unterstützen die Festlegung der geeigneten Management-Aktionen und Prioritäten für das Management von Informationssicherheitsrisiken, und für die Umsetzung der Maßnahmen, die zum Schutz gegen diese Risiken ausgewählt wurden.

Die Risikoeinschätzung sollte regelmäßig wiederholt werden, um alle Veränderungen zu berücksichtigen, die die Ergebnisse der Risikoeinschätzung beeinflussen können.

Weitere Informationen über die Einschätzung von Informationssicherheitsrisiken befinden sich in 4.1 „Einschätzen der Sicherheitsrisiken“.

0.5 Auswahl von Maßnahmen

Nachdem die Sicherheitsanforderungen und Risiken identifiziert und die Entscheidungen für die Risikobehandlung getroffen wurden, sollten angemessene Maßnahmen ausgewählt und umgesetzt werden, um sicherzustellen, dass die Risiken auf ein akzeptables Level reduziert werden. Maßnahmen können aus dieser Norm oder anderen Maßnahmenkatalogen ausgewählt werden. Bei Bedarf können auch neue Maßnahmen entwickelt werden, um spezifische Anforderungen zu erfüllen. Die Auswahl von Sicherheitsmaßnahmen ist abhängig von den Entscheidungen, die die Organisation basierend auf den Kriterien für die Risikoakzeptanz, den Möglichkeiten der Risikobehandlung und dem allgemeinen Risikomanagement-Ansatz der Organisation getroffen hat. Diese Auswahl sollte auch alle relevanten nationalen und internationalen Gesetze und Vorschriften berücksichtigen.

Einige der Maßnahmen in dieser Norm können als Richtlinien für Informationssicherheits-Management verstanden werden, und sind für die meisten Organisationen anwendbar. Diese Maßnahmen sind unten unter „Ausgangspunkt für Informationssicherheit“ näher ausgeführt.

Weitere Informationen über die Auswahl von Maßnahmen und anderen Risikobehandlungsoptionen befinden sich in 4.2 „Behandeln der Sicherheitsrisiken“.

0.6 Ausgangspunkt für Informationssicherheit

Eine Anzahl von Maßnahmen kann als geeigneter Ausgangspunkt für die Umsetzung von Informationssicherheit betrachtet werden. Diese basieren entweder auf wesentlichen gesetzlichen Anforderungen oder sind in der Informationssicherheit allgemein üblich.

Zu den Maßnahmen, die vom gesetzlichen Standpunkt aus gesehen von wesentlicher Bedeutung für eine Organisation sind (falls diese Gesetze zutreffen), gehören:

- a) Datenschutz und Vertraulichkeit von personenbezogenen Informationen (siehe 15.1.4);
- b) Schutz von organisationsinternen Aufzeichnungen (siehe 15.1.3);
- c) Urheberrechte (siehe 15.1.2).

Zu den Maßnahmen, die für Informationssicherheit als allgemein üblich angesehen werden, gehören:

- a) Informationssicherheitsleitlinie (siehe 5.1.1);
- b) Zuweisung von Verantwortlichkeiten für Informationssicherheit (siehe 6.1.3);
- c) Sensibilisierung, Ausbildung und Schulung für Informationssicherheit (siehe 8.2.2);
- d) korrekte Verarbeitung in Anwendungen (siehe 12.2);
- e) Schwachstellenmanagement (siehe 12.6);
- f) Management des kontinuierlichen Geschäftsbetriebs (siehe Abschnitt 14);
- g) Management von Informationssicherheitsvorfällen und Verbesserungen (siehe 13.2).

Diese Maßnahmen sind in den meisten Organisationen und Umgebungen anwendbar.

Obwohl alle Maßnahmen in dieser Norm wichtig sind und betrachtet werden sollten, wird darauf hingewiesen, dass die Bedeutung einer Maßnahme in Abhängigkeit von den spezifischen Risiken bestimmt werden sollte, denen sich eine Organisation gegenübersteht. Auch wenn der oben dargestellte Ansatz als guter Ausgangspunkt angesehen werden kann, kann er eine auf einer Risikoeinschätzung basierende Auswahl von Maßnahmen nicht ersetzen.

0.7 Entscheidende Erfolgsfaktoren

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

- a) Informationssicherheitsgrundsätze, -ziele und -aktivitäten, die die Geschäftsziele widerspiegeln;
- b) ein Ansatz und Rahmen für die Umsetzung Betrieb, Überwachung und Verbesserung von Informationssicherheit, der mit der Organisationskultur vereinbar ist;
- c) sichtbare Unterstützung und Engagement von allen Ebenen des Managements;
- d) gutes Verständnis der Anforderungen an Informationssicherheit, Risikoeinschätzung und Risikomanagement;

- e) effektives Marketing von Informationssicherheit gegenüber allen Managern, Mitarbeitern und sonstigen Parteien, um Bewusstsein zu bilden;
- f) Verteilung von Anleitungen für die Informationssicherheitsleitlinie und Normen an alle Manager, Mitarbeiter und sonstige Parteien;
- g) Vorkehrung zur Finanzierung von Aktivitäten für Informationssicherheits-Management;
- h) Bereitstellung eines angemessenen Sensibilisierungs-, Ausbildungs- und Schulungsprogramms zur Verbesserung des Sicherheitsbewusstseins;
- i) Einrichtung eines effektiven Prozesses zum Management von Informationssicherheitsvorfällen;
- j) Umsetzung eines Messsystems¹⁾ zur Leistungsbeurteilung beim Informationssicherheits-Management und zur Rückmeldung von Verbesserungsvorschlägen.

0.8 Entwicklung eigener Richtlinien

Dieser Leitfaden darf als Ausgangspunkt für die Entwicklung organisationsspezifischer Richtlinien angesehen werden. Unter Umständen sind nicht alle Maßnahmen und Anleitungen aus dieser Norm anwendbar. Darüber hinaus können zusätzliche Maßnahmen und Richtlinien erforderlich sein, die nicht in dieser Norm enthalten sind. Wenn Dokumente mit zusätzlichen Richtlinien oder Maßnahmen entwickelt werden, kann es sich als nützlich erweisen, Querverweise zu diesem Standard zu integrieren, die die Prüfung der Einhaltung der Norm durch Auditoren und Geschäftspartner erleichtern.

¹⁾ Das Messen von Informationssicherheit ist außerhalb des Geltungsbereichs dieses Standards.

1 Anwendungsbereich

Diese Internationale Norm legt Leitlinien und allgemeine Prinzipien für die Initiierung, Umsetzung, den Betrieb und die Verbesserung des Informationssicherheits-Managements in einer Organisation fest. Die in dieser Norm beschriebenen Ziele liefern eine generelle Anleitung für die allgemein anerkannte Zielsetzung für Informationssicherheits-Management.

Die Maßnahmenziele und Maßnahmen in dieser Internationalen Norm sollen umgesetzt werden, um die im Rahmen einer Risikoeinschätzung identifizierten Anforderungen zu erfüllen. Dabei soll diese Internationale Norm als praktische Richtlinie für das Entwickeln organisationseigener Sicherheitsstandards und wirksamer Sicherheitsmanagementpraktiken gelten und soll helfen, das Vertrauen in Geschäftsbeziehungen zwischen Organisationen aufzubauen.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1

Wert

alles, was für die Organisation von Wert ist

[ISO/IEC 13335-1:2004]

2.2

Maßnahme

Mittel für das Risikomanagement, einschließlich Leitlinien, Verfahren, Richtlinien, Praktiken oder organisationseigene Strukturen, welche verwaltender, technischer, leitender oder gesetzlicher Natur sein können

ANMERKUNG Der Begriff „Maßnahme“ wird auch als Synonym zu „Schutzmaßnahme“ und „Gegenmaßnahme“ verwendet.

2.3

Richtlinie

Beschreibung, die klarstellt, was wie getan werden soll, um die in der Leitlinie formulierten Ziele zu erreichen

[ISO/IEC 13335-1:2004]

2.4

informationsverarbeitende Einrichtungen

alle informationsverarbeitenden Systeme, Dienstleistungen oder Infrastrukturen, oder die physischen Standorte, an denen diese untergebracht sind

2.5

Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden

2.6

Informationssicherheitsereignis

erkanntes Auftreten eines System-, Service- oder Netzzustands, der einen möglichen Verstoß gegen die Informationssicherheitsleitlinie oder Fehler von Maßnahmen, oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt

[ISO/IEC TR 18044:2004]

2.7**Informationssicherheitsvorfall**

einzelnes oder Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird

[ISO/IEC TR 18044:2004]

2.8**Leitlinie**

vom Management formell ausgedrückte Gesamtintention und -richtung

2.9**Risiko**

Kombination aus Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen

[ISO/IEC Guide 73:2002]

2.10**Risikoanalyse**

systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos

[ISO/IEC Guide 73:2002]

2.11**Risikoeinschätzung**

gesamter Prozess der Risikoanalyse und Risikobewertung

[ISO/IEC Guide 73:2002]

2.12**Risikobewertung**

Prozess, in dem das eingeschätzte Risiko mit den festgelegten Kriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen

[ISO/IEC Guide 73:2002]

2.13**Risikomanagement**

koordinierte Aktivitäten zur Leitung und Kontrolle einer Organisation in Bezug auf Risiken

ANMERKUNG Risikomanagement beinhaltet normalerweise Risikoeinschätzung, Risikobehandlung, Risikoakzeptanz und Risikokommunikation.

[ISO/IEC Guide 73:2002]

2.14**Risikobehandlung**

Prozess für die Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos

[ISO/IEC Guide 73:2002]

2.15**Dritte**

natürliche oder juristische Person, die von den involvierten Parteien für die fragliche Angelegenheit als unabhängig angesehen wird

[ISO/IEC Guide 2:1996]

2.16

Bedrohung

mögliche Ursache eines Vorfalles, der einem System oder einer Organisation einen Schaden zufügen kann

[ISO/IEC 13335-1:2004]

2.17

Schwachstelle

von einer oder mehreren Bedrohungen ausnutzbare Schwäche eines Wertes oder einer Gruppe von Gütern

[ISO/IEC 13335-1:2004]

3 Aufbau dieser Norm

Diese Norm enthält 11 Abschnitte mit Sicherheitsmaßnahmen, die zusammen insgesamt 39 wesentliche Sicherheitskategorien enthalten, und einen einleitenden Abschnitt, der die Themen Risikoeinschätzung und Risikobehandlung vorstellt.

3.1 Abschnitte

Jeder Abschnitt enthält eine Anzahl von wesentlichen Sicherheitskategorien. Die 11 Abschnitte (zusammen mit der Anzahl der in diesem Abschnitt enthaltenen wesentlichen Sicherheitskategorien) sind:

- a) Sicherheitsleitlinie (1);
- b) Organisation der Informationssicherheit (2);
- c) Management von organisationseigenen Werten (2);
- d) Sicherheit im Personalbereich (3);
- e) physische und umgebungsbezogene Sicherheit (2);
- f) Management der Kommunikation und des Betriebs (10);
- g) Zugangskontrolle (7);
- h) Beschaffung, Entwicklung und Wartung von Informationssystemen (6);
- i) Management von Informationssicherheitsvorfällen (2);
- j) Aufrechterhaltung des Geschäftsbetriebs (1);
- k) Einhaltung von Verpflichtungen (3).

ANMERKUNG Die Reihenfolge der Abschnitte in dieser Norm impliziert nicht deren Wichtigkeit. In Abhängigkeit von den Umständen können alle Abschnitte wichtig sein. Daher sollte jede Organisation, die diese Norm anwendet, die für sie relevanten Abschnitte bestimmen und einschätzen wie wichtig diese und deren Anwendung für die individuellen Geschäftsprozesse sind. Auch die Aufzählungen in dieser Norm sind nicht nach Priorität geordnet, sofern dies nicht angegeben ist.

3.2 Wesentliche Sicherheitskategorien

Jede der wesentlichen Sicherheitskategorien enthält

- a) ein Maßnahmenziel, das angibt, was zu erreichen ist, und

- b) eine oder mehrere Maßnahmen, die angewandt werden können, um dieses Maßnahmenziel zu erreichen.

Die Beschreibung der Maßnahmen ist wie folgt strukturiert:

Maßnahme

Definiert die spezifische Aussage der Maßnahme zur Erfüllung des Maßnahmenziels.

Anleitung zur Umsetzung

Stellt weitere detaillierte Informationen bereit, um die Umsetzung der Maßnahmen und das Erreichen des Maßnahmenziels zu unterstützen. Manche der Anleitungen sind möglicherweise nicht in allen Fällen passend. Daher können andere Wege der Umsetzung der Maßnahme geeigneter sein.

Weitere Informationen

Stellt weitere Informationen bereit, die möglicherweise zu berücksichtigen sind, zum Beispiel Überlegungen im Hinblick auf Gesetze oder Verweise auf andere Standards.

4 Risikoeinschätzung und -behandlung

4.1 Einschätzung der Sicherheitsrisiken

Eine Risikoeinschätzung sollte Risiken nach Kriterien für Risikoakzeptanz und relevanten Zielen der Organisation identifizieren, quantifizieren und priorisieren. Die Ergebnisse sollten die geeigneten Aktionen des Managements und Prioritäten für den Umgang mit Informationssicherheitsrisiken und für die Auswahl von Maßnahmen zum Schutz gegen diese Risiken lenken und bestimmen. Der Prozess der Risikoeinschätzung und der Auswahl von Maßnahmen muss gegebenenfalls mehrmals durchlaufen werden, um verschiedene Teile der Organisation oder individuelle Informationssysteme zu behandeln.

Die Risikoeinschätzung sollte einen systematischen Ansatz zur Einschätzung des Ausmaßes von Risiken (Risikoanalyse) enthalten, und einen Prozess zum Vergleich der abgeschätzten Risiken nach Risikokriterien, um die Signifikanz der Risiken zu bestimmen (Risikobewertung).

Risikoeinschätzungen sollten außerdem regelmäßig durchgeführt werden, um Veränderungen der Sicherheitsanforderungen und der Risikosituation zu berücksichtigen. Solche Veränderungen können sich beispielsweise in den Werten, Bedrohungen, Schwachstellen, Auswirkungen und der Risikobewertung ergeben, und wenn wesentliche Änderungen auftreten. Diese Risikoeinschätzungen sollten systematisch durchgeführt werden, um vergleichbare und reproduzierbare Ergebnisse zu erzeugen.

Um wirkungsvoll zu sein, sollte die Einschätzung der Informationssicherheitsrisiken einen klar definierten Anwendungsbereich haben, und sie sollte, sofern es angemessen ist, die Beziehungen zu den Risikoeinschätzungen in anderen Gebieten mit einbeziehen.

Der Anwendungsbereich einer Risikoeinschätzung kann entweder die ganze Organisation, Teile der Organisation, ein einzelnes Informationssystem, spezifische Systemkomponenten oder Dienstleistungen sein, wenn dies praktikabel, realistisch und hilfreich ist. Beispiele für Methoden zur Risikoeinschätzung werden in ISO/IEC TR 13335-3 (*Information technology – Guidelines for the management of IT security – Part 3: Techniques for the managing of IT security*) diskutiert.

4.2 Umgang mit Sicherheitsrisiken

Bevor die Behandlung eines Risikos in Erwägung gezogen wird, sollte die Organisation Kriterien bestimmen, mit deren Hilfe entschieden werden kann, ob Risiken akzeptiert werden können oder nicht. Risiken dürfen akzeptiert werden, wenn zum Beispiel das Risiko als niedrig eingeschätzt wird, oder wenn die Kosten einer Risikobehandlung für die Organisation nicht wirtschaftlich vertretbar sind. Solche Entscheidungen sollten dokumentiert werden.

Für jedes der identifizierten Risiken muss eine Entscheidung getroffen werden, wie damit umzugehen ist. Mögliche Optionen für den Umgang mit Risiken sind:

- a) Anwendung von geeigneten Maßnahmen zur Reduktion von Risiken;
- b) Bewusstes und tatsächliches Akzeptieren der Risiken, sofern sie eindeutig den Leitlinien der Organisation und den Kriterien für eine Risikoakzeptanz genügen;
- c) Vermeidung spezieller Risiken durch Untersagen von Aktionen, die diese Risiken verursachen würden;
- d) Übertragung der zugehörigen Geschäftsrisiken auf andere Parteien, wie zum Beispiel Versicherer oder Lieferanten.

Für die Risiken, für die laut Risikobehandlungsentscheidung geeignete Maßnahmen angewandt werden sollen, sollten diese Maßnahmen ausgewählt und umgesetzt werden, um die Anforderungen zu erfüllen, die durch die Risikoeinschätzung identifiziert wurden. Maßnahmen sollten sicherstellen, dass Risiken auf ein akzeptables Niveau reduziert werden, und dabei Folgendes berücksichtigen:

- a) Anforderungen und Einschränkungen durch nationale und internationale Gesetze und Bestimmungen;
- b) organisationseigene Ziele;
- c) betriebliche Anforderungen und Einschränkungen;
- d) Kosten für die Umsetzung und den Betrieb im Verhältnis zu den zu reduzierenden Risiken, und um den Anforderungen und Einschränkungen der Organisation zu entsprechen;
- e) die Erfordernis, die Ausgaben für die Umsetzung und den Betrieb der Maßnahmen gegen den Schaden abzuwägen, der vermutlich durch Sicherheitsprobleme entsteht.

Maßnahmen können aus dieser Norm oder aus anderen Sammlungen von Maßnahmen gewählt werden. Es können auch neue Maßnahmen entwickelt werden, um die spezifischen Anforderungen der Organisation zu erfüllen. Dabei sollte man sich darüber im Klaren sein, dass einige Maßnahmen nicht für jedes Informationssystem oder für jede Umgebung anwendbar sind, und dass sie vielleicht nicht für alle Organisationen praktikabel sind. Beispielsweise wird in 10.1.3 beschrieben, wie Aufgaben aufgeteilt werden können, um Betrug und Fehler zu vermeiden. Kleinere Organisationen sind eventuell nicht in der Lage, alle Aufgaben aufzuteilen, so dass andere Wege erforderlich sein können, um dasselbe Maßnahmenziel zu erreichen. Als weiteres Beispiel beschreibt 10.10, wie die Systemnutzung überwacht und Beweise gesammelt werden können. Die dort beschriebenen Maßnahmen, z. B. das Aufzeichnen von Ereignissen, könnten in Konflikt mit geltenden Gesetzen stehen, wie zum Beispiel dem Datenschutz für Kunden oder am Arbeitsplatz.

Bei der Erstellung der System- und Projekt-Anforderungen (Pflichtenheft) sowie während der Entwicklung sollten Informationssicherheitsmaßnahmen berücksichtigt werden. Andernfalls kann dies zu zusätzlichen Kosten und zu weniger effektiven Lösungen führen. Schlimmstenfalls wird es unmöglich, angemessene Sicherheit zu erreichen.

Es sollte berücksichtigt werden, dass durch keine Zusammenstellung von Maßnahmen absolute Sicherheit erreicht werden kann. Daher sollten zusätzliche Managementaktionen umgesetzt werden, um die Leistungsfähigkeit und die Wirksamkeit von Sicherheitsmaßnahmen zu überwachen, zu bewerten und zu verbessern. Dies dient dem Zweck die Ziele der Organisation zu unterstützen.

5 Sicherheitsleitlinie

5.1 Informationssicherheitsleitlinie

Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen.

Das Management sollte eine klare Richtung der Grundsätze in Einklang mit Geschäftszielen vorgeben und Unterstützung und Engagement für Informationssicherheit durch organisationsweite Veröffentlichung und Aufrechterhaltung einer Informationssicherheitsleitlinie vorgeben.

5.1.1 Leitlinie zur Informationssicherheit

Maßnahme

Das Management sollte eine Informationssicherheitsleitlinie genehmigen, veröffentlichen und alle Angestellten und relevanten Externen davon in Kenntnis setzen.

Anleitung zur Umsetzung

Die Informationssicherheitsleitlinie sollte das Engagement des Managements ausdrücken und den Ansatz der Organisation für das Management der Informationssicherheit darstellen. Das Dokument sollte Angaben zu den folgenden Aspekten enthalten:

- a) eine Definition der Informationssicherheit, ihrer allgemeinen Ziele und ihres Anwendungsbereichs, sowie die Bedeutung der Sicherheit als Mittel, einen Informationsaustausch überhaupt zu ermöglichen (siehe Einleitung);
- b) eine Absichtserklärung des Managements, Ziele und Prinzipien der Informationssicherheit in Einklang mit der Geschäftsstrategie und den Geschäftszielen zu unterstützen;
- c) einen Rahmen für die Festlegung von Maßnahmenzielen und Maßnahmen, einschließlich der Struktur von Risikoeinschätzung und Risikomanagement;
- d) eine kurze Erläuterung der Sicherheitsleitlinien, Prinzipien, Standards und einzuhaltenden Anforderungen, die von besonderer Bedeutung für die Organisation sind, inklusive:
 - 1) Einhaltung der gesetzlichen, behördlichen und vertraglichen Anforderungen;
 - 2) Anforderungen an Sicherheitsausbildung, Training und Sensibilisierung in Sachen Informationssicherheit;
 - 3) Aufrechterhaltung des Geschäftsbetriebs;
 - 4) Konsequenzen bei Verstößen gegen die Sicherheitspolitik;
- e) eine Definition allgemeiner und spezifischer Verantwortlichkeiten für Informationssicherheitsmanagement, einschließlich der Meldung von Informationssicherheitsvorfällen;
- f) Verweise auf Dokumente, die die Politik unterstützen dürfen, z. B. ausführlichere Sicherheitsleitlinien und -verfahren für spezifische Informationssysteme oder von den Benutzern einzuhaltende Sicherheitsregeln.

Diese Informationssicherheitsleitlinie sollte in einer sachdienlichen, zugänglichen und verständlichen Form an alle Benutzer in der Organisation kommuniziert werden.

Weitere Informationen

Die Informationssicherheitsleitlinie kann Teil eines allgemeinen Regelwerkes sein. Wenn die Informationssicherheitsleitlinie außerhalb der Organisation verteilt wird, sollte sichergestellt werden, dass keine sensiblen Informationen weitergegeben werden. Weitere Informationen können in ISO/IEC 13335-1:2004 gefunden werden.

5.1.2 Überprüfung der Informationssicherheitsleitlinie

Maßnahme

Die Informationssicherheitsleitlinie sollte in regelmäßigen Abständen und immer dann überprüft werden, wenn wesentliche Änderungen erfolgen, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.

Anleitung zur Umsetzung

Die Informationssicherheitsleitlinie sollte einen Eigentümer haben, der die vom Management übertragene Verantwortung für die Entwicklung, Überprüfung und Bewertung der Sicherheitsleitlinie hat. Die Überprüfung sollte eine Beurteilung der Möglichkeiten zur Verbesserung der Informationssicherheitspolitik beinhalten. Zudem sollte der Ansatz zum Umgang mit den Aspekten der Informationssicherheit daraufhin überprüft werden, inwiefern Änderungen der Geschäftsbedingungen, der gesetzlichen Rahmenbedingungen oder des technischen Umfelds berücksichtigt werden müssen.

Die Überprüfung der Informationssicherheitsleitlinie sollte die Ergebnisse aus durchgeführten Managementbewertungen berücksichtigen. Es sollte festgelegte Verfahren zur Managementbewertung geben, die einen Zeitplan oder Fristen für die Bewertung beinhalten.

Die folgenden Punkte sollten Eingang in die Managementbewertung finden:

- a) Rückmeldungen von betroffenen Parteien;
- b) Ergebnisse aus unabhängigen Überprüfungen (siehe 6.1.8);
- c) Status der vorbeugenden und korrigierenden Maßnahmen (siehe 6.1.8 und 15.2.1);
- d) Ergebnisse von vorhergehenden Managementbewertungen;
- e) Durchführung von Prozessen und Einhaltung der Informationssicherheitsleitlinie;
- f) Änderungen, die den Ansatz der Organisation für das Management von Informationssicherheit beeinflussen können, einschließlich Änderungen im organisationseigenen Umfeld, geschäftlichen Umständen, Verfügbarkeit von Ressourcen, von vertraglichen, behördlichen oder gesetzlichen Gegebenheiten, oder im technischen Umfeld;
- g) Entwicklungen bei Bedrohungen und Schwachstellen;
- h) Berichte über Informationssicherheitsvorfälle (siehe 13.1);
- i) Empfehlungen von maßgeblichen Behörden (siehe 6.1.6).

Die Ergebnisse der Managementbewertung sollten alle Entscheidungen und Aktionen in Zusammenhang mit den folgenden Punkten beinhalten:

- a) Verbesserung des Ansatzes der Organisation für das Management von Informationssicherheit und der Prozesse;
- b) Verbesserung von Maßnahmenzielen und Maßnahmen;
- c) Verbesserung in der Zuweisung von Ressourcen und/oder Verantwortlichkeiten.

Aufzeichnungen der Managementbewertung sollten gepflegt werden.

Die Zustimmung des Managements zu der überarbeiteten Leitlinie sollte eingeholt werden.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Handhabung der Informationssicherheit innerhalb der Organisation.

Ein Managementrahmen sollte geschaffen werden, um die Umsetzung der Informationssicherheit innerhalb der Organisation einzuführen und zu steuern.

Das Management sollte die Informationssicherheitsleitlinie genehmigen, sicherheitsbezogene Aufgaben zuweisen und die Umsetzung der Informationssicherheit organisationsweit koordinieren und überprüfen.

Bei Bedarf sollten spezifische Informationssicherheitsratschläge bereitgestellt und innerhalb der Organisation verfügbar gemacht werden. Kontakte zu externen Sicherheitsfachkräften oder -gruppen, einschließlich relevanter Behörden, sollten hergestellt werden, um mit industriellen Trends Schritt zu halten, Normen und Bewertungsmethoden zu überwachen sowie geeignete Anlaufstellen zur Behandlung von Sicherheitsvorfällen zu schaffen. Eine interdisziplinäre Vorgehensweise bei der Informationssicherheit sollte gefördert werden.

6.1.1 Engagement des Managements für Informationssicherheit

Maßnahme

Das Management sollte die Informationssicherheit innerhalb der Organisation aktiv unterstützen, indem es eine klare Ausrichtung vorgibt, sein Engagement demonstriert, Aufgaben explizit formuliert und die Verantwortlichkeiten für Informationssicherheit anerkennt.

Anleitung zur Umsetzung

Das Management sollte:

- a) sicherstellen, dass die Informationssicherheitsziele identifiziert werden, die Anforderungen der Organisation erfüllen und in die relevanten Prozesse integriert werden;
- b) die Informationssicherheitsleitlinie formulieren, überprüfen und genehmigen;
- c) die Wirksamkeit der Umsetzung der Informationssicherheitsleitlinie überprüfen;
- d) eine klare Ausrichtung vorgeben und Sicherheitsinitiativen sichtbar unterstützen;
- e) die für Informationssicherheit benötigten Ressourcen bereitstellen;
- f) die Zuweisung von spezifischen Aufgaben und Verantwortlichkeiten für Informationssicherheit organisationsweit genehmigen;
- g) Pläne und Programme initiieren, um das Bewusstsein für Informationssicherheit aufrechtzuerhalten;
- h) sicherstellen, dass die Umsetzung von Informationssicherheitsmaßnahmen organisationsweit koordiniert wird (siehe 6.1.2).

Das Management sollte den Bedarf an Beratung durch interne oder externe Fachleute für Informationssicherheit identifizieren und die Ergebnisse daraus überprüfen und organisationsweit die sich daraus ergebenden Aktivitäten koordinieren.

Je nach Größe der Organisation kann diese Verantwortung von einem eigenen Managementforum oder einem bereits vorhandenen Managementgremium, wie dem Vorstand, wahrgenommen werden.

Weitere Informationen

Weitere Informationen dazu enthält ISO/IEC 13335-1:2004.

6.1.2 Koordination der Informationssicherheit

Maßnahme

Aktivitäten im Rahmen der Informationssicherheit sollten durch Repräsentanten verschiedener Organisationsbereiche mit relevanten Aufgabenbereichen und Funktionen koordiniert werden.

Anleitung zur Umsetzung

Üblicherweise sollte die Koordination der Informationssicherheit die Mitwirkung und Zusammenarbeit von Managern, Benutzern, Systemadministratoren, Anwendungsdesignern, Auditoren und Sicherheitspersonal, sowie Fachleute aus Bereichen wie z. B. Versicherungswesen, Recht, Personal, IT oder Risikomanagement einbeziehen. Diese Aktivität sollte:

- a) sicherstellen, dass die Sicherheitsaktivitäten in Übereinstimmung mit der Informationssicherheitsleitlinie ausgeführt werden;
- b) festlegen, wie Verstöße behandelt werden sollen;
- c) Methodiken und Prozesse für Informationssicherheit genehmigen, z. B. Risikoeinschätzung, Klassifizierung von Informationen;
- d) wesentliche Änderungen in den Bedrohungen und die Art der Bedrohung, der Informationen und informationsverarbeitende Einrichtungen ausgesetzt sind, identifizieren;
- e) die Angemessenheit von Informationssicherheitsmaßnahmen einschätzen und deren Umsetzung koordinieren;
- f) die Ausbildung, das Training und die Sensibilisierung für die Aspekte der Informationssicherheit organisationsweit wirksam fördern;
- g) die durch die Überwachung und Überprüfung von Informationssicherheitsvorfällen erhaltenen Informationen auswerten, und angemessene Aktionen als Antwort auf identifizierte Informationssicherheitsvorfälle empfehlen.

Falls die Organisation keine separate funktionsübergreifende Gruppe einsetzt, z. B. weil eine solche Gruppe für die Größe der Organisation nicht angemessen ist, sollten die oben beschriebenen Aktionen durch ein anderes geeignetes Managementgremium oder einen einzelnen Manager wahrgenommen werden.

6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit

Maßnahme

Alle Verantwortlichkeiten für Informationssicherheit sollten eindeutig definiert sein.

Anleitung zur Umsetzung

Die Zuweisung der Verantwortlichkeiten für Informationssicherheit sollte in Einklang mit der Informationssicherheitsleitlinie (siehe Abschnitt 4) geschehen. Die Verantwortlichkeiten für den Schutz einzelner Werte und für die Durchführung spezifischer Sicherheitsprozesse sollten eindeutig definiert sein. Sie sollten im Bedarfsfall durch ausführlichere Anleitungen für spezifische Standorte und informationsverarbeitende Einrichtungen ergänzt werden. Ortsspezifische Verantwortlichkeiten für den Schutz von Werten und für die Durchführung spezifischer Sicherheitsprozesse, z. B. Planung zur Aufrechterhaltung des Geschäftsbetriebs, sollten eindeutig definiert sein.

Personen, denen Sicherheitsverantwortung zugewiesen wurde, dürfen Sicherheitsaufgaben an andere Personen delegieren. Sie bleiben aber dennoch verantwortlich und sollten überprüfen, dass alle delegierten Aufgaben korrekt ausgeführt wurden.

Die Verantwortungsbereiche von Personen sollten klar festgelegt werden; insbesondere sollte Folgendes stattfinden:

- a) für jedes System sollten die zugehörigen Werte und Sicherheitsprozesse identifiziert und eindeutig definiert werden;

- b) allen organisationseigenen Werten (Assets) sowie den Sicherheitsprozessen sollte ein entsprechender Verantwortlicher zugewiesen werden und die Details dieser Verantwortung sollten dokumentiert werden (siehe auch 7.1.2);
- c) Berechtigungen sollten eindeutig definiert und dokumentiert werden.

Weitere Informationen

In vielen Organisationen wird ein Informationssicherheitsmanager ernannt, der die Gesamtverantwortung für die Entwicklung und Umsetzung von Sicherheit übernimmt und die Identifizierung von Maßnahmen unterstützt.

Allerdings verbleibt die Verantwortung für die Bereitstellung von Ressourcen und die Umsetzung von Maßnahmen häufig bei dem jeweiligen Manager. Eine verbreitete Vorgehensweise ist die Ernennung eines Eigentümers für jeden Wert, der dann für dessen tägliche Sicherheit verantwortlich ist.

6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen

Maßnahme

Für neue informationsverarbeitende Einrichtungen sollte ein Genehmigungsverfahren durch das Management festgelegt und umgesetzt werden.

Anleitung zur Umsetzung

Die folgenden Regelungen für Genehmigungsverfahren sollten betrachtet werden:

- a) neue Einrichtungen sollten die entsprechende Genehmigung durch das Management erfahren haben, das deren Zweck und Einsatz genehmigt. Es sollte auch eine Zustimmung des Managers eingeholt werden, der für die Wartung der lokalen Informationssystem-Sicherheitsumgebung verantwortlich ist, um die Erfüllung aller relevanten Sicherheitsleitlinien und -anforderungen sicherzustellen;
- b) bei Bedarf sollten Hardware und Software geprüft werden, um die Kompatibilität mit anderen Systemkomponenten sicherzustellen;
- c) die Verwendung von persönlichen oder privaten informationsverarbeitenden Geräten, z. B. Laptops, Heimcomputer oder tragbare Geräte/PDA, für die Verarbeitung von Geschäftsinformationen kann neue Schwachstellen hervorrufen und erforderliche Maßnahmen sollten identifiziert und umgesetzt werden.

6.1.5 Vertraulichkeitsvereinbarungen

Maßnahme

Anforderungen an Vertraulichkeitsvereinbarungen oder zur Geheimhaltung, die den Schutzbedarf der Organisation für Informationen widerspiegeln, sollten identifiziert und regelmäßig überprüft werden.

Anleitung zur Umsetzung

Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollten die Anforderungen, vertrauliche Informationen zu schützen, in juristisch einklagbaren Formulierungen adressieren. Um die Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen zu identifizieren, sollten die folgenden Punkte betrachtet werden:

- a) Definition der zu schützenden Informationen (z. B. vertrauliche Informationen);
- b) erwartete Dauer der Vereinbarung, einschließlich der Fälle, wo Vertraulichkeit vielleicht unbegrenzt gewahrt bleiben muss;
- c) notwendige Aktionen, wenn die Vereinbarung beendet ist;
- d) Verantwortlichkeiten und Aktionen der Unterzeichnenden, um die unberechtigte Weitergabe von Informationen zu vermeiden (z. B. Beschränkung auf das Nötigste);
- e) Eigentum von Informationen, Geschäftsgeheimnissen und Urheberrechten, und in welchem Verhältnis dies zum Schutz vertraulicher Informationen steht;

- f) der zulässige Gebrauch von vertraulichen Informationen, sowie die Rechte des Unterzeichnenden, diese Informationen zu benutzen;
- g) das Recht, die Aktivitäten, die vertrauliche Informationen betreffen zu überwachen und aufzuzeichnen;
- h) Melde- und Berichtsprozess bei unberechtigter Weitergabe oder Verletzung der Vertraulichkeit von Informationen;
- i) Bedingungen für die Rückgabe oder Vernichtung von Informationen, wenn die Verpflichtung endet; und
- j) erwartete Aktionen, die im Fall eines Verstoßes gegen die Verpflichtung ergriffen werden.

Abhängig von den Sicherheitsanforderungen einer Organisation können andere Elemente in einer Vertraulichkeits- oder Geheimhaltungsvereinbarungen notwendig sein.

Vertraulichkeits- und Geheimhaltungsvereinbarungen sollten im Einklang mit allen relevanten Gesetzen und Bestimmungen ihres Einfluss- und Anwendungsbereichs sein (siehe auch 15.1.1).

Anforderungen an Vertraulichkeits- und Geheimhaltungsvereinbarungen sollten regelmäßig, und immer dann, wenn Änderungen auftreten, die diese Regelungen beeinflussen, überprüft werden.

Weitere Informationen

Vertraulichkeits- und Geheimhaltungsvereinbarungen schützen die Informationen einer Organisation und informieren die Unterzeichnenden über ihre Verpflichtung, die Informationen in verantwortlicher und berechtigter Weise zu schützen, zu benutzen und weiterzugeben.

In einer Organisation kann Bedarf bestehen, unter verschiedenen Umständen unterschiedliche Formen von Vertraulichkeits- und Geheimhaltungsvereinbarungen zu benutzen.

6.1.6 Kontakt zu Behörden

Maßnahme

Geeigneter Kontakt zu relevanten Behörden sollten gepflegt werden.

Anleitung zur Umsetzung

Organisationen sollten klare Vorgehensweisen etabliert haben, die beschreiben, wann und durch wen Behörden (z. B. Strafverfolgung, Feuerwehr, Aufsichtsbehörden) kontaktiert werden sollten, und wie festgestellte Informationssicherheitsvorfälle unverzüglich berichtet werden sollten, wenn vermutet wird, dass diese gegen Gesetze verstoßen.

Organisationen, die über das Internet angegriffen werden, sind eventuell darauf angewiesen, dass Externe (z. B. ein Internetdienstanbieter oder Telekommunikationsbetreiber) Maßnahmen gegen den Urheber des Angriffs unternehmen.

Weitere Informationen

Die Pflege solcher Kontakte darf gefordert werden, um die Bearbeitung von Informationssicherheitsvorfällen (13.2) oder den Planungsprozess für Notfälle und zum Aufrechterhalten des Geschäftsbetriebs (Abschnitt 14) zu unterstützen. Kontakte mit Regulierungsbehörden können ebenfalls nützlich sein, um bevorstehende Änderungen in Gesetzen oder Vorschriften, denen die Organisation unterliegt, vorwegzunehmen und sich darauf vorzubereiten. Kontakte mit anderen Behörden beinhalten Versorgungsunternehmen, Rettungsdienste, und Gesundheit und Sicherheit, z. B. Feuerwehr (in Zusammenhang mit der Aufrechterhaltung des Geschäftsbetriebs), Telekommunikationsbetreiber (in Zusammenhang mit Leitungsbereitstellung und Verfügbarkeit), Wasserterversorgung (in Zusammenhang mit Kühlungsanlagen für Geräte).

6.1.7 Kontakt zu speziellen Interessengruppen

Maßnahme

Geeignete Kontakte zu speziellen Interessengruppen oder anderen Experten-Sicherheitsforen und professionellen Verbänden sollten gepflegt werden.

Anleitung zur Umsetzung

Die Mitgliedschaft in speziellen Interessengruppen oder Foren sollte in Betracht gezogen werden, um:

- a) das Wissen über empfohlene Methoden (Best Practice) zu erweitern und bezüglich relevanter Sicherheitsinformationen auf dem Laufenden zu bleiben;
- b) sicherzustellen, dass das Verständnis der Informationssicherheitsumgebung aktuell und vollständig ist;
- c) frühzeitig Hinweise auf Alarme und Sicherheitsgefährdungen, auf Sicherheitsmaßnahmen, und auf Patches gegen Angriffe und Schwachstellen zu erhalten;
- d) Zugang zu spezifischen Informationssicherheitsanleitungen zu erhalten;
- e) Informationen über neue Technologien, Produkte, Bedrohungen oder Schwachstellen zu teilen und auszutauschen;
- f) Schnittstellen für die Zusammenarbeit bei der Behandlung von Informationssicherheitsvorfällen (siehe auch 13.2.1) bereitzustellen.

Weitere Informationen

Vereinbarungen über den Informationsaustausch können etabliert werden, um die Kooperation und Koordination von Sicherheitsfragen zu verbessern. Diese Regelungen sollten den Schutzbedarf sensibler Informationen festlegen.

6.1.8 Unabhängige Überprüfung der Informationssicherheit

Maßnahme

Der Ansatz einer Organisation zur Handhabung und Umsetzung der Informationssicherheit (d. h. Maßnahmenziele, Maßnahmen, Leitlinien, Prozesse und Verfahren für Informationssicherheit) sollte in regelmäßigen Zeitabständen, oder nach wesentlichen Änderungen an der implementierten Sicherheit von unabhängiger Seite überprüft werden.

Anleitung zur Umsetzung

Die unabhängige Prüfung sollte vom Management veranlasst werden. Solch eine unabhängige Überprüfung ist notwendig, um die ständige Eignung, Angemessenheit und Wirksamkeit des Ansatzes der Organisation für die Handhabung der Informationssicherheit zu gewährleisten. Die Überprüfung sollte auch die Untersuchung von Möglichkeiten zur Verbesserung und Untersuchungen des Bedarfs für Änderungen am generellen Ansatz für Sicherheit, einschließlich der Leitlinie und der Maßnahmenziele beinhalten.

Eine derartige Überprüfung sollte durch Personen ausgeführt werden, die unabhängig von dem zu überprüfenden Bereich sind, z. B. die interne Revision, interne Auditoren, eine unabhängige Führungskraft oder eine externe Organisation, die auf solche Prüfungen spezialisiert ist. Personen, die diese Überprüfungen durchführen, sollten die erforderlichen Fähigkeiten und Erfahrungen besitzen.

Die Ergebnisse der unabhängigen Überprüfung sollten aufgezeichnet und dem Management berichtet werden, das die Überprüfung veranlasst hat. Diese Aufzeichnungen sollten aktuell gehalten werden.

Falls die unabhängige Überprüfung ergibt, dass der Ansatz und die Umsetzung der Organisation für die Handhabung von Informationssicherheit nicht angemessen sind oder nicht konform mit der Ausrichtung der Informationssicherheit, wie sie in der Informationssicherheitsleitlinie festgelegt ist (siehe 5.1.1), sollte das Management Korrekturen des Vorgehens in Betracht ziehen.

Weitere Informationen

Der Bereich, den Manager regelmäßig überprüfen sollten (siehe 15.2.1), darf auch von unabhängiger Seite überprüft werden. Überprüfungsverfahren dürfen Interviews des Managements, die Kontrolle von Aufzeichnungen oder die Durchsicht von Sicherheitsleitlinien sein. ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*, kann ebenfalls eine hilfreiche Anleitung zur Durchführung einer unabhängigen Überprüfung, einschließlich der Erstellung und Umsetzung eines Überprüfungsprogramms liefern. 15.3 beschreibt Maßnahmen, die sich auf die unabhängige Überprüfung von im Betrieb befindlichen Informationssystemen und den Gebrauch von Tools für Systemaudits beziehen.

6.2 Externe

Ziel: Aufrechterhaltung der Sicherheit von Informationen und von informationsverarbeitenden Einrichtungen der Organisation, die von Externen benutzt oder verwaltet werden, die für diese zugänglich sind, oder die an Externe kommuniziert werden.

Die Sicherheit von Informationen und informationsverarbeitenden Einrichtungen der Organisation sollte durch die Einführung von Produkten oder Dienstleistungen von Externen nicht beeinträchtigt werden.

Jeglicher Zugang, den Externe zu den informationsverarbeitenden Einrichtungen haben sowie die Verarbeitung und Kommunikation von Informationen durch Externe sollte überwacht werden.

Wenn es geschäftliche Gründe für die Zusammenarbeit mit Externen gibt, die dazu eventuell auch Zugang zu den Informationen und informationsverarbeitenden Einrichtungen der Organisation benötigen, oder wenn eine Dienstleistung oder ein Produkt von Externen bereitgestellt oder ihnen zur Verfügung gestellt wird, so sollte eine Risikoeinschätzung durchgeführt werden, um die Auswirkungen auf die Sicherheit und die Anforderungen an die erforderlichen Maßnahmen zu ermitteln. Maßnahmen sollten mit Externen vereinbart und in einem Vertrag fixiert werden.

6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern

Maßnahme

Die Risiken für Informationen und informationsverarbeitende Einrichtungen der Organisation, die durch Geschäftsprozesse unter Beteiligung Externer verursacht werden, sollten identifiziert und angemessene Maßnahmen umgesetzt werden, bevor diesen der Zugriff gewährt wird.

Anleitung zur Umsetzung

Wenn Externe Zugriff auf Informationen oder informationsverarbeitende Einrichtungen der Organisation benötigen, sollte eine Risikoeinschätzung (siehe auch Abschnitt 4) durchgeführt werden, um alle Anforderungen für spezifische Maßnahmen zu identifizieren. Die Identifizierung der Risiken in Zusammenhang mit Externen sollte die folgenden Punkte mitberücksichtigen:

- a) die informationsverarbeitenden Einrichtungen, auf die Externe zugreifen müssen;
- b) die Art des Zugriffs, die Externe auf die Informationen und informationsverarbeitende Einrichtungen haben werden, z. B.:
 - 1) physischer Zugang, z. B. zu Büros, Computerräumen, Aktenschränken;
 - 2) logischer Zugang, z. B. zu den Datenbanken oder Informationssystemen einer Organisation;
 - 3) Verbindungen zwischen Netzen der Organisation und Netzen der externen Partei, z. B. Festverbindungen, Fernzugriff;
 - 4) ob der Zugang vor Ort oder von außerhalb der Organisation stattfindet;
- c) den Wert und die Sensitivität der involvierten Informationen, und deren Kritikalität für den Geschäftsbetrieb;

- d) die notwendigen Maßnahmen zum Schutz derjenigen Informationen, die für Externe nicht zugänglich sein sollen;
- e) die Mitarbeiter der externen Partei, die in die Bearbeitung von organisationseigenen Informationen involviert sind;
- f) wie zugangs- und zugriffsberechtigte Organisationen oder Mitarbeiter identifiziert werden können, wie die Berechtigung verifiziert werden kann, und wie häufig dies bestätigt werden muss;
- g) die verschiedenen Mittel und Maßnahmen, die Externe bei der Speicherung, Verarbeitung, Kommunikation und Weitergabe, sowie beim Austausch von Informationen einsetzen;
- h) die Auswirkungen, wenn Externen kein Zugang bei Bedarf zur Verfügung steht, und wenn Externe inkorrekte oder irreführende Informationen eingeben oder erhalten;
- i) Praktiken und Verfahren, um mit Informationssicherheitsvorfällen und möglichen Schäden umzugehen, und die Bedingungen für weiteren Zugang für Externe nach Informationssicherheitsvorfällen;
- j) gesetzliche und behördliche Anforderungen und andere vertragliche Verpflichtungen, die im Zusammenhang mit Externen zu berücksichtigen sind;
- k) die Frage, wie die Interessen anderer Stakeholder durch diese Regelungen beeinträchtigt werden könnten.

Externen sollte der Zugang zu den Informationen der Organisation erst dann bereitgestellt werden, wenn geeignete Maßnahmen umgesetzt wurden, und – falls praktikabel – ein Vertrag unterzeichnet wurde, der die Bedingungen für die Verbindung oder den Zugang und die Nutzung definiert. Im Allgemeinen sollten sich alle aus der Zusammenarbeit mit Externen oder aus den betrieblichen Kontrollen resultierenden Sicherheitsanforderungen in vertraglichen Regelungen mit der externen Partei (siehe auch 6.2.2 und 6.2.3) widerspiegeln.

Es sollte sichergestellt werden, dass sich Externe ihrer Verpflichtungen bewusst sind und die Verantwortlichkeiten und Haftung akzeptieren, die der Zugriff, die Verarbeitung, die Kommunikation oder die Verwaltung von Informationen und informationsverarbeitenden Einrichtungen mit sich bringen.

Weitere Informationen

Informationen können durch Externe, bei einem unzureichenden Sicherheitsmanagement, von externer Seite gefährdet sein. Maßnahmen sollten identifiziert und umgesetzt werden, um den Zugang Externen zu informationsverarbeitenden Einrichtungen zu verwalten. Wenn zum Beispiel eine besondere Notwendigkeit besteht, dass Informationen vertraulich behandelt werden, so können Vertraulichkeitsvereinbarungen abgeschlossen werden.

Eine Organisation kann mit Risiken in Zusammenhang mit Prozessen, Management und Kommunikation zwischen Organisationen konfrontiert werden, wenn ein hohes Maß an Outsourcing (Auslagerung) angewandt wird oder wenn mehrere externe Parteien involviert sind.

Die Maßnahmen 6.2.2 und 6.2.3 decken Vereinbarungen mit unterschiedlichen externen Parteien ab, z. B.:

- a) Dienstleister, z. B. ISPs, Netzdienstleister, Telefonservices, Dienstleister für Wartung und Support;
- b) Sicherheitsdienstleister (Managed Security Services);
- c) Kunden;
- d) Auslagerung von Einrichtungen und/oder Abläufen, z. B. IT-Systeme, Datenerfassungsdienste, Call-Center-Betrieb;
- e) Management- und Wirtschaftsberater und Revisoren;
- f) Entwickler und Zulieferer, z. B. von Softwareprodukten und IT-Systemen;

- g) Reinigungsfirmen, Kantinenbetrieb und andere ausgelagerte Dienstleitungen;
- h) vorübergehend beschäftigte Mitarbeiter, Einstellung von Studenten und andere zeitlich befristete Anstellungen.

Solche Vereinbarungen können helfen, die Risiken in Zusammenhang mit Externen zu reduzieren.

6.2.2 Adressieren von Sicherheit im Umgang mit Kunden

Maßnahme

Alle identifizierten Sicherheitsanforderungen sollten berücksichtigt sein, bevor Kunden Zugang zu Informationen oder Werten der Organisation gegeben wird.

Anleitung zur Umsetzung

Die folgenden Bedingungen sollten berücksichtigt werden, um Sicherheitsaspekten gerecht zu werden, bevor einem Kunden der Zugang zu Werten der Organisation ermöglicht wird (je nach Art und Ausführung des gewählten Zugangs treffen gegebenenfalls nicht alle Bedingungen zu):

- a) Schutz von Werten, einschließlich:
 - 1) Verfahren um die Werte der Organisation (Assets), einschließlich Informationen und Software zu schützen, und der Umgang mit bekannten Schwachstellen;
 - 2) Verfahren, um festzustellen, ob die organisationseigenen Werte (Assets) in irgendeiner Weise kompromittiert wurden, z. B. in Form von Datenverlust oder -veränderung;
 - 3) Integrität;
 - 4) Einschränkungen bzgl. des Kopierens und der Freigabe von Informationen;
- b) Beschreibung des zur Verfügung gestellten Produkts oder der bereitgestellten Dienstleistung;
- c) die verschiedenen Gründe, Anforderungen und Vorteile des Kundenzugangs;
- d) Richtlinie zur Zugangskontrolle, einschließlich:
 - 1) zulässige Zugangsmethoden, und die Kontrolle und Benutzung eindeutiger Kennungen, wie Benutzerkennungen und Passwörter;
 - 2) ein Berechtigungsprozess für Benutzerzugang und Privilegien;
 - 3) eine Erklärung, dass jeglicher Zugang verboten ist, der nicht ausdrücklich erlaubt ist;
 - 4) einen Prozess, Zugangs- und Zugriffsrechte zu entziehen oder die Verbindung zwischen Systemen zu unterbrechen;
- e) Vereinbarungen für Berichte, Mitteilungen und Untersuchungen von Ungenauigkeiten der Informationen (z. B. persönliche Details), von Informationssicherheitsvorfällen und Sicherheitsverstößen;
- f) eine Beschreibung jeder bereitgestellten Dienstleistung;
- g) der angestrebte Service-Level und nicht akzeptable Service-Levels;
- h) das Recht, jegliche Aktivitäten in Zusammenhang mit den Werten der Organisation (Assets) zu überwachen und zu widerrufen;
- i) die Haftungsregelungen zwischen der Organisation und dem Kunden;

- j) Verantwortlichkeiten zur Gesetzeskonformität, und Sicherstellung der Erfüllung gesetzlicher Anforderungen, z. B. Datenschutzgesetze; insbesondere unter Berücksichtigung verschiedener nationaler Rechtssysteme, wenn die Vereinbarung die Zusammenarbeit mit Kunden im Ausland einschließt (siehe auch 15.1);
- k) geistiges Eigentum und die Zuweisung von Urheberrechten (siehe 15.1.2), sowie der Schutz jeglicher gemeinschaftlicher Arbeit (siehe auch 6.1.5).

Weitere Informationen

Die Sicherheitsanforderungen, die sich daraus ergeben, dass Kunden auf Werte der Organisation (Assets) zugreifen können, in Abhängigkeit davon, auf welche informationsverarbeitenden Einrichtungen und auf welche Informationen zugegriffen wird, stark variieren. Diesen Sicherheitsanforderungen kann man durch Kundenvereinbarungen gerecht werden, die alle identifizierten Risiken und Sicherheitsanforderungen (siehe 6.2.1) behandeln.

Vereinbarungen mit Externen dürfen auch andere Parteien einbeziehen. Vereinbarung, die externen Parteien Zugang und Zugriff erlauben, sollten diesen die Erlaubnis einräumen andere zulässige Parteien auszuwählen, und Bedingungen für deren Zugang und deren Einbeziehung festschreiben.

6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten

Maßnahme

Vereinbarungen mit Dritten, die den Zugriff, die Verarbeitung, Kommunikation oder Administration von Informationen oder informationsverarbeitenden Einrichtungen der Organisation betreffen, oder die Bereitstellung von Produkten oder Dienstleistungen für informationsverarbeitende Einrichtungen, sollten alle relevanten Sicherheitsanforderungen abdecken.

Anleitung zur Umsetzung

Die Vereinbarung sollte sicherstellen, dass keinerlei Missverständnisse zwischen der Organisation und dem Dritten bestehen. Organisationen sollten angemessenen Schadensersatz durch Dritte sicherstellen.

Die Aufnahme der folgenden Bedingungen in der Vereinbarung sollte erwogen werden, um die identifizierten Sicherheitsanforderungen (siehe 6.2.1) zu erfüllen:

- a) die Informationssicherheitsleitlinie;
- b) Maßnahmen zur Sicherstellung des Schutzes von organisationseigenen Werten (Assets), einschließlich:
 - 1) Verfahren zum Schutz organisationseigener Werte (Assets), einschließlich Informationen, Software und Hardware;
 - 2) alle notwendigen Maßnahmen und Mechanismen für den physischen Schutz;
 - 3) Maßnahmen, die den Schutz vor bösartigen Codes sicherstellen (siehe 10.4.1);
 - 4) Verfahren zur Bestimmung, ob eine Kompromittierung von Werten stattgefunden hat, z. B. in Form von Verlust oder Veränderung der Informationen, Software und Hardware;
 - 5) Maßnahmen, um die Rückgabe oder Vernichtung von Informationen und Werten bei Vertragsende oder zu einem vereinbarten Zeitpunkt innerhalb der Vertragslaufzeit sicherzustellen;
 - 6) Vertraulichkeit, Integrität, Verfügbarkeit und alle anderen wichtigen Eigenschaften von organisationseigenen Werten (siehe 2.1.5);
 - 7) Einschränkungen bzgl. des Kopierens und der Freigabe von Informationen sowie die Verwendung von Vertraulichkeitsverpflichtungen (siehe 6.1.5);

- c) Benutzer- und Administratorschulung in Methoden, Verfahren und Sicherheit;
- d) sicherstellen, dass die Benutzer ihrer Verantwortung für Informationssicherheit bewusst sind;
- e) gegebenenfalls Vorkehrungen für die Übernahme von Personal;
- f) Verantwortlichkeiten in Bezug auf Installation und Wartung von Hardware und Software;
- g) eine eindeutige Berichtsstruktur und festgelegte Berichtsformate;
- h) ein eindeutiger und festgelegter Prozess für die Handhabung von Anpassungen;
- i) Richtlinie zur Zugangskontrolle, einschließlich:
 - 1) die unterschiedlichen Gründe, Anforderungen und Vorteile, die den Zugang von Dritten notwendig machen;
 - 2) zulässige Zugangsmethoden, und die Kontrolle und Benutzung eindeutiger Kennungen wie Benutzerkennungen und Passwörtern;
 - 3) ein Berechtigungsprozess für Benutzerzugriff und -privilegien;
 - 4) die Anforderung, eine Liste zu pflegen, welche Personen zur Benutzung der zur Verfügung gestellten Dienste berechtigt sind, und welches ihre Rechte und Privilegien im Rahmen dieser Benutzung sind;
 - 5) eine Erklärung, dass jeglicher Zugang verboten ist, der nicht ausdrücklich erlaubt ist;
 - 6) einen Prozess, Zugangs- und Zugriffsrechte zu entziehen oder die Verbindung zwischen Systemen zu unterbrechen;
- j) Vereinbarungen für Berichte, Mitteilungen und Untersuchungen von Informationssicherheitsvorfällen und Sicherheitsverstößen, genauso wie Vertragsverstöße;
- k) eine Beschreibung des bereitgestellten Produkts oder der Dienstleistung, und eine Beschreibung der zur Verfügung gestellten Informationen, einschließlich ihrer Sicherheitsklassifizierung (siehe 7.2.1);
- l) das angestrebte Service-Level und nicht akzeptable Service-Levels;
- m) die Definition überprüfbarer Leistungskriterien, deren Überwachung und Berichterstattung;
- n) das Recht, jegliche Aktivitäten in Zusammenhang mit den Werten der Organisation zu überwachen und zu widerrufen;
- o) das Recht, die vertraglich festgelegten Verantwortlichkeiten zu überprüfen, diese Prüfungen durch unabhängige Dritte durchführen zu lassen, und die satzungsgemäßen Rechte der Prüfer zu benennen;
- p) Einrichtung eines Eskalationsprozesses zur Problemlösung;
- q) Anforderungen an die Kontinuität der Dienstleistung, einschließlich von Messgrößen für Verfügbarkeit und Verlässlichkeit, die im Einklang mit den geschäftlichen Prioritäten der Organisation sind;
- r) die vereinbarte Verpflichtung der jeweiligen Parteien;
- s) Verantwortlichkeiten zur Gesetzeskonformität, und Sicherstellung der Erfüllung gesetzlicher Anforderungen, z. B. Datenschutzgesetze; insbesondere unter Berücksichtigung unterschiedlicher nationaler Rechtssysteme, wenn die Vereinbarung die Zusammenarbeit mit Organisationen im Ausland einschließt (siehe auch 15.1);

- t) geistiges Eigentum und die Zuweisung von Urheberrechten (siehe 15.1.2), und der Schutz von jeglicher gemeinschaftlicher Arbeit (siehe auch 6.1.5).
- u) Einbeziehung Dritter mit Subunternehmern, sowie die Sicherheitsmaßnahmen, die diese Subunternehmer umsetzen müssen;
- v) Bedingungen für die Neuverhandlung/Beendigung von Vereinbarungen:
 - 1) für den Fall, dass eine Partei die Geschäftsbeziehung vor Vertragslaufzeitende beenden möchte, sollte ein Notfallplan existieren;
 - 2) Neuverhandlung von Vereinbarungen, wenn sich die Sicherheitsanforderungen der Organisation ändern;
 - 3) laufende Dokumentation von Listen über organisationseigene Werte, Lizenzen, Vereinbarungen oder die daraus resultierenden Rechte.

Weitere Informationen

Vereinbarungen können für verschiedene Organisationen und für unterschiedliche Arten von Dritten beträchtlich variieren. Daher sollte dafür gesorgt werden, dass alle identifizierten Risiken und Sicherheitsanforderungen (siehe auch 6.2.1) vertraglich berücksichtigt werden. Gegebenenfalls können die erforderlichen Maßnahmen und Verfahren in einem Sicherheitsmanagementplan weiter ausgeführt werden.

Bei ausgelagertem Informationssicherheits-Management sollten die Vereinbarungen darauf eingehen, wie Dritte ein angemessenes Sicherheitsniveau sicherstellen können, wie durch die Risikoeinschätzung definiert, und wie dieses Sicherheitsniveau angepasst wird, um einem veränderten Risiko gerecht zu werden.

Einige der Unterschiede zwischen Outsourcing und anderen Formen der Bereitstellung von Dienstleistungen durch Dritte betreffen Haftungsfragen, die Planung des Übergangszeitraums und der möglichen Unterbrechungen des Betriebs während dieses Zeitraums, Arrangements für Notfallplanung und Überprüfung der notwendigen Sorgfalt, und die Erfassung und das Management von Informationen über Sicherheitsvorfälle. Daher ist es wichtig, dass die Organisation den Übergang zu einem Outsourcing-Vertrag plant und steuert, und dass geeignete Verfahren zur Handhabung von Änderungen und zur Neuverhandlung/Beendigung von Vereinbarungen existieren.

Für den Fall, dass Dritte außer Stande sind, zugesagte Dienstleistungen zu erbringen, sollten Übergangsregelungen in der Vereinbarung enthalten sein, um einen reibungslosen Wechsel zu einem Ersatzdienstleister sicherzustellen.

Vereinbarungen mit Dritten können auch andere Parteien einschließen. Vereinbarungen, die externen Parteien Zugang und Zugriff erlauben, sollten diesen die Erlaubnis einräumen andere berechnigte Parteien auszuwählen, und Bedingungen für deren Zugang und Beteiligung festschreiben.

Normalerweise werden Vereinbarungen vornehmlich von der Organisation entwickelt. Unter Umständen kann eine Vereinbarung von Dritten entwickelt und der Organisation vorgeschrieben werden. Die Organisation muss dann sicherstellen, dass ihre eigene Sicherheit nicht unnötigerweise durch die derart auferlegten Anforderungen Dritter beeinflusst wird.

7 Management von organisationseigenen Werten

7.1 Verantwortung für organisationseigene Werte (Assets)

Ziel: Erreichen und Erhaltung eines angemessenen Schutzes von organisationseigenen Werten (Assets).

Alle organisationseigenen Werte (Assets) sollten einer Person zugerechnet werden können und einen benannten Eigentümer haben.

Für alle organisationseigenen Werte (Assets) sollten Eigentümer bestimmt werden, denen die Verantwortung für die Bereitstellung angemessener Maßnahmen obliegt. Im Einzelfall kann der Eigentümer die Umsetzung bestimmter Maßnahmen delegieren; er bleibt aber verantwortlich für den angemessenen Schutz der Werte.

7.1.1 Inventar der organisationseigenen Werte (Assets)

Maßnahme

Alle organisationseigenen Werte (Assets) sollten eindeutig identifiziert und ein Inventar aller wichtigen organisationseigenen Werte (Assets) erstellt und gepflegt werden.

Anleitung zur Umsetzung

Eine Organisation sollte alle organisationseigenen Werte (Assets) identifizieren und die Bedeutung dieser Werte dokumentieren. Das Inventar der organisationseigenen Werte (Assets) sollte alle Informationen enthalten, die zur Wiederherstellung nach einer Katastrophe nötig sind, einschließlich der Art des Wertes, Format, Ort, Backup-Informationen, Lizenzinformationen und des Geschäftswerts. Das Inventar sollte nicht unnötigerweise andere Inventare kopieren, ein Abgleich der Inhalte sollte aber sichergestellt sein.

Außerdem sollten für jeden der organisationseigenen Werte (Assets) Eigentümerschaft (siehe 7.1.2) und Klassifizierung der Informationen (siehe 7.2) vereinbart und dokumentiert sein. Basierend auf der Wichtigkeit der organisationseigenen Werte (Assets), ihres Geschäftswerts und ihrer Sicherheitsklassifizierung sollte ein angemessener Grad von Schutz identifiziert werden, der die Wertigkeit widerspiegelt (weitere Informationen über die Bewertung von organisationseigenen Werten (Assets) zur Festlegung ihrer Wertigkeit können in ISO/IEC TR 13335-3 gefunden werden).

Weitere Informationen

Es gibt viele Arten von organisationseigenen Werten (Assets), zum Beispiel:

- a) Informationen: Datenbanken und Dateien, Verträge und Vereinbarungen, Systemdokumentation, Forschungsinformationen, Benutzerhandbücher, Schulungsunterlagen, Betriebs- oder Supportverfahren, Kontinuitätspläne, Sicherungsarrangements, Auditprotokolle und archivierte Informationen;
- b) Software: Anwendungssoftware, Systemsoftware, Entwicklungstools und Dienstprogramme;
- c) physische Werte: Computeranlagen, Kommunikationsanlagen, Datenträger und andere technische Ausstattung (Netzgeräte, Klimageräte), Möbel, Räumlichkeiten;
- d) Dienstleistungen: Rechner- und Kommunikationsdienste, allgemeine Versorgungsleistungen (z. B. Heizung, Licht, Strom und Klimaanlage);
- e) Personen, und ihre Qualifikationen, Fähigkeiten und Erfahrung;
- f) immaterielle Werte, wie der gute Ruf und Image der Organisation.

Inventare von organisationseigenen Werten (Assets) helfen sicherzustellen, dass die Werte effektiv geschützt werden. Sie dürfen auch für andere Geschäftszwecke erforderlich sein, z. B. aus Gesundheits- und Sicherheitsgründen, versicherungstechnischen oder finanziellen Gründen (Werteverwaltung). Die Erstellung eines Inventars von organisationseigenen Werten (Assets) ist eine wichtige Voraussetzung für das Risikomanagement (siehe auch Abschnitt 4).

7.1.2 Eigentum von organisationseigenen Werten (Assets)

Maßnahme

Alle Informationen und organisationseigenen Werte (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen sollten Eigentum²⁾ eines bestimmten Teils der Organisation sein.

Anleitung zur Umsetzung

Der Eigentümer eines Wertes sollte verantwortlich sein für die:

- a) Sicherstellung, dass Informationen und Werte in Verbindung mit informationsverarbeitenden Einrichtungen angemessen klassifiziert werden;
- b) Definition und regelmäßige Überprüfung der Zugangs-/Zugriffsbeschränkungen und Klassifikation der Werte, unter Berücksichtigung der anwendbaren Zugangskontrollpolitiken.

Eigentum darf zugewiesen werden für:

- a) einen Geschäftsprozess;
- b) eine bestimmte Gruppe von Aktivitäten;
- c) eine Anwendung; oder
- d) einen bestimmten Datensatz.

Weitere Informationen

Routineaufgaben dürfen delegiert werden, z. B. an einen Betreuer, der sich täglich um den Wert kümmert, die Verantwortung verbleibt aber beim Eigentümer.

In komplexen Informationssystemen kann es nützlich sein, Gruppen von organisationseigenen Werten (Assets) zu bestimmen, die zusammenwirken, um eine bestimmte Funktion als Dienst zu erfüllen. In diesem Fall ist der Eigentümer des Dienstes verantwortlich für die Bereitstellung des Dienstes, was das Funktionieren der zugehörigen Werte beinhaltet.

7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets)

Maßnahme

Regeln für den zulässigen Gebrauch von Informationen und organisationseigenen Werten (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen sollten identifiziert, dokumentiert und umgesetzt werden.

Anleitung zur Umsetzung

Alle Mitarbeitern, Vertragsnehmer und Drittbenutzer ^{N1)} sollten den Regeln für den zulässigen Gebrauch von Informationen und organisationseigenen Werten (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen folgen, einschließlich:

- a) Regeln für E-Mail und Internetbenutzung (siehe 10.8);
- b) Regelungen für den Gebrauch von mobilen Geräten, insbesondere für den Gebrauch außerhalb des Firmengeländes (siehe 11.7.1);

2) Der Begriff „Eigentümer“ bezeichnet eine natürliche oder juristische Person, die die vom Management zugewiesene Verantwortung für die Kontrolle von Produktion, Entwicklung, Pflege, Gebrauch und Sicherheit der Werte hat. Der Begriff „Eigentümer“ bedeutet nicht, dass diese Person irgendwelche Eigentumsrechte an diesem Wert hat.

N1) Nationale Fußnote: Siehe 8.1 für eine Erklärung dieser Begriffe.

Entsprechende Regeln oder Anleitungen sollte das zuständige Management zur Verfügung stellen. Mitarbeiter, Vertragsnehmer und Drittbenutzer, die die Werte der Organisation benutzen oder Zugang zu ihnen haben, sollten sich der existierenden Auflagen für die Benutzung organisationseigener Informationen und Werte in Verbindung mit informationsverarbeitenden Einrichtungen und Ressourcen bewusst sein. Sie sollten für den Gebrauch jeglicher informationsverarbeitender Einrichtungen verantwortlich sein, und für jeglichen Gebrauch, der unter ihrer Verantwortung ausgeführt wird.

7.2 Klassifizierung von Informationen

Ziel: Sicherstellung des angemessenen Schutzes von Informationen.

Informationen sollten klassifiziert werden, um den Bedarf, die Prioritäten und den erwarteten Umfang des Schutzes bei der Nutzung von Informationen angeben zu können.

Informationen können einen unterschiedlichen Grad von Sensitivität und Wichtigkeit haben. Manche Elemente können einen zusätzlichen Schutz oder eine besondere Handhabung erfordern. Ein Klassifikationsschema für Informationen sollte zur Anwendung kommen, das ein angemessenes Maß an Schutzniveaus definiert und den Bedarf an spezifischen Maßnahmen zur Handhabung ausdrückt.

7.2.1 Regelungen für die Klassifizierung

Maßnahme

Informationen sollten bezüglich ihres Werts, gesetzlicher Anforderungen, ihrer Sensitivität und ihrer Kritikalität für die Organisation klassifiziert werden.

Anleitung zur Umsetzung

Klassifizierungen und damit verbundene Maßnahmen für Informationen sollten sicherstellen, dass die Geschäftsanforderungen für die gemeinsame oder eingeschränkte Nutzung von Informationen sowie die mit solchen Anforderungen verbundenen geschäftlichen Folgen berücksichtigt werden.

Regelungen zur Klassifizierung sollten Vorgaben für die erstmalige Klassifizierung und eine erneute Klassifizierung nach einer bestimmten Frist beinhalten, in Übereinstimmung mit einem vorher festgelegten Zugangskontroll-Regelwerk (siehe 11.1.1).

Der Eigentümer des Assets/unternehmerischen Wertes (siehe 7.1.2) sollte dafür verantwortlich sein, die Klassifizierung des Wertes vorzunehmen, sie regelmäßig zu überprüfen, und sicherzustellen, dass sie aktuell und auf dem richtigen Level gehalten wird. Die Klassifizierung sollte den in 10.7.2 erwähnten Aggregationseffekt berücksichtigen.

Die Anzahl der Klassifizierungskategorien und die Vorteile, die aus ihrer Nutzung erwachsen, sollten gründlich überlegt sein. Übermäßig komplexe Schemata könnten sich in der Praxis als schwerfällig, unwirtschaftlich oder unanwendbar erweisen. Einstufungsbezeichnungen auf Dokumenten anderer Organisationen sollten mit Vorsicht interpretiert werden, da andere Organisationen andere Definitionen für dieselbe oder eine ähnlich lautende Klassifikationsstufe haben könnten.

Weitere Informationen

Das Schutzniveau kann durch die Analyse der Vertraulichkeits-, Integritäts-, Verfügbarkeits- und beliebiger anderer Anforderungen an die betrachteten Informationen bestimmt werden.

Nach einem bestimmten Zeitraum, z. B. nach Veröffentlichung der Informationen, sind die Informationen häufig nicht mehr sensitiv oder kritisch. Dies sollte berücksichtigt werden, da eine zu hohe Klassifizierung die Umsetzung von unnötigen Maßnahmen mit zusätzlichen Kosten mit sich bringen kann.

Die gemeinsame Einstufung von Dokumenten mit ähnlichen Sicherheitsanforderungen bei der Zuweisung von Klassifizierungslevels kann die Aufgabe vereinfachen.

Die einer Information zugewiesene Klassifizierung ist im Allgemeinen eine einfache Methode, um die Handhabung und den Schutz für diese Information festzulegen.

7.2.2 Kennzeichnung von und Umgang mit Informationen

Maßnahme

Geeignete Verfahren für die Kennzeichnung von und den Umgang mit Informationen sollten in Übereinstimmung mit dem von der Organisation angewandten Klassifizierungsschema entwickelt und umgesetzt werden.

Anleitung zur Umsetzung

Verfahren für die Kennzeichnung von Informationen müssen Informationswerte in physischer und elektronischer Form berücksichtigen.

Ergebnisse von Systemen mit als sensitiv oder kritisch klassifizierten Informationen sollten entsprechend ihrer Klassifikation (wie in 7.2.1 festgelegt) gekennzeichnet sein. Die Kennzeichnung sollte gedruckte Berichte, Bildschirmausgaben, magnetische Datenträger (z. B. Bänder, Disketten, CDs), elektronische Nachrichten (E-Mail) und Datentransfer berücksichtigen.

Für jeden Klassifizierungslevel sollten Verfahren zum Umgang definiert werden, welche die sichere Verarbeitung, Speicherung, Übertragung, Deklassifizierung und Vernichtung enthalten. Dies sollte auch Verfahren für die Beweissicherung und die Protokollierung sicherheitsrelevanter Ereignisse einschließen.

Verträge mit anderen Organisationen, die die gemeinsame Nutzung von Informationen beinhalten, sollten Verfahren enthalten, um die Klassifizierung dieser Informationen zu bestimmen, und um die Klassifizierungslevels anderer Organisationen umzusetzen.

Weitere Informationen

Kennzeichnung und sichere Handhabung von klassifizierten Informationen ist eine entscheidende Anforderung für Vereinbarungen zur gemeinsamen Informationsnutzung. Physische Kennzeichnungen sind dazu eine gebräuchliche Form. Einige Informationswerte, z. B. Dokumente in elektronischer Form, lassen sich jedoch nicht physisch kennzeichnen und müssen elektronisch gekennzeichnet werden. Hinweise dürfen zum Beispiel auf dem Bildschirm oder Display angezeigt werden. Falls eine Kennzeichnung nicht machbar ist, dürfen andere Mittel angewandt werden, um die Klassifizierung von Informationen zu bestimmen, z. B. mittels Verfahren oder Meta-Daten.

8 Personalsicherheit

8.1 Vor der Anstellung³⁾

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer^{N2)} ihre Verantwortlichkeiten verstehen und für die vorgesehenen Aufgaben geeignet sind, und um die Risiken durch Diebstahl, Betrug oder Missbrauch von Einrichtungen zu verringern.

Die Verantwortung für Sicherheit sollte vor der Einstellung in entsprechenden Tätigkeitsbeschreibungen und Arbeitsvertragsregelungen behandelt werden.

Alle Bewerber für eine Anstellung, Auftragnehmer und Drittbenutzer sollten angemessen überprüft werden, insbesondere, wenn sie sensitive Tätigkeiten ausführen sollen.

Angestellte, Auftragnehmer und Drittbenutzer von informationsverarbeitenden Einrichtungen sollten eine Verpflichtung auf ihre Sicherheitsaufgaben und -verantwortlichkeiten unterschreiben.

3) Erklärung: Der Begriff „Anstellung“ wird hier benutzt, um die folgenden verschiedenen Situationen zu behandeln: Anstellung von Personen (kurzzeitig oder länger andauernd), Zuweisung von Arbeitsaufgaben, Ändern von Arbeitsaufgaben, Zuordnung von Verträgen, und die Beendigung dieser Arrangements.

N2) Nationale Fußnote: Erklärung: Die hier verwandten Begriffe bezeichnen folgende Situationen:

1. Auftragnehmer: Hier sind alle Personen gemeint, deren Arbeit bei der Organisation über einen Vertrag geregelt ist, sie aber nicht Angestellte der Organisation sind. Beispiele sind unabhängige Berater oder durch Agenturen vermitteltes Personal.
2. Drittbenutzer: Dies bezeichnet alle Benutzer, die bei Dritten unter Vertrag stehen (siehe auch 6.2).

8.1.1 Aufgaben und Verantwortlichkeiten

Maßnahme

Sicherheitsaufgaben und -verantwortlichkeiten von Angestellten, Auftragnehmern und Drittbenutzern sollten im Einklang mit den Informationssicherheitsgrundsätzen der Organisation definiert und dokumentiert werden.

Anleitung zur Umsetzung

Sicherheitsaufgaben und -verantwortlichkeiten sollten die folgenden Anforderungen enthalten:

- a) Umsetzung und Agieren im Einklang mit den Informationssicherheitsgrundsätzen der Organisation (siehe 5.1);
- b) Schutz von Werten vor unberechtigtem Zugriff, Offenlegung, Veränderung, Zerstörung oder Beeinträchtigung;
- c) Ausführung besonderer Sicherheitsprozesse oder Aktivitäten;
- d) sicherstellen, dass Personen für die von ihnen durchgeführten Aktivitäten verantwortlich sind;
- e) berichten von Sicherheitsereignissen oder potentiellen Ereignissen, oder anderen Sicherheitsrisiken für die Organisation.

Sicherheitsaufgaben und -Verantwortlichkeiten sollten definiert und Bewerbern während des Auswahlprozesses klar mitgeteilt werden.

Weitere Informationen

Tätigkeitsbeschreibungen können benutzt werden, um Sicherheitsaufgaben und -verantwortlichkeiten zu dokumentieren. Sicherheitsaufgaben und -verantwortlichkeiten von Personen, die nicht durch den organisationseigenen Einstellungsprozess ausgewählt werden, z. B. von Dritten bereitgestellt werden, sollten ebenfalls eindeutig definiert und kommuniziert werden.

8.1.2 Überprüfung

Maßnahme

Überprüfungen der Vergangenheit aller Bewerber, Auftragnehmer und Drittbenutzer sollten in Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen ausgeführt werden, und sollten den Geschäftsanforderungen, der Klassifizierung der Informationen, die diese verwenden werden, und den erkannten Risiken angemessen sein.

Anleitung zur Umsetzung

Überprüfungen sollten alle relevanten Gesetze zu den Themen Datenschutz und/oder Arbeitsrecht berücksichtigen, und sollten, falls zulässig, die folgenden Punkte beinhalten:

- a) Vorhandensein ausreichender Referenzen, z. B. eine geschäftlicher und eine persönlicher Natur;
- b) Überprüfung des Lebenslaufs des Bewerbers (auf Vollständigkeit und Richtigkeit);
- c) Bestätigung der angegebenen akademischen und beruflichen Qualifikationen;
- d) unabhängige Identitätsprüfung (Reisepass oder ähnliches Dokument);
- e) weiterführende Prüfungen, wie Überprüfung der Kreditwürdigkeit oder Prüfung auf Vorstrafen (polizeiliches Führungszeugnis).

Wenn immer es eine Aufgabe, bei Anstellung oder Beförderung, mit sich bringt, dass die Person Zugang zu informationsverarbeitenden Einrichtungen hat, und insbesondere dann, wenn diese sensitive Informationen,

z. B. finanzielle Informationen oder sehr vertrauliche Informationen, enthalten, sollte die Organisation weitere, detailliertere Prüfungen in Betracht ziehen.

Verfahren sollten Kriterien und Grenzen für Überprüfungen definieren, z. B. wer zur Personenüberprüfung qualifiziert ist, und wann, wie und warum Nachprüfungen durchgeführt werden.

Für Auftragnehmer und Drittbenutzer sollte ebenfalls ein Überprüfungsprozess eingeführt werden. Falls Auftragnehmer durch eine Agentur bereitgestellt werden, sollten die Verantwortlichkeiten der Agentur für eine Überprüfung eindeutig festgelegt werden, ebenso die Informationspflicht, wenn die Überprüfung noch nicht abgeschlossen wurde oder die Ergebnisse Anlass zu Bedenken oder Besorgnis geben. Gleicherweise sollte die Vereinbarung mit Dritten (siehe auch 6.2.3) die Verantwortlichkeiten und Informationspflicht für eine Überprüfung eindeutig festlegen.

Informationen über die Bewerber für Positionen in der Organisation sollten in Übereinstimmung mit allen einschlägigen Gesetzen, gesammelt und verarbeitet werden. Abhängig von den anwendbaren Gesetzen sollte die Zustimmung der Bewerber vor einer Überprüfung eingeholt werden.

8.1.3 Arbeitsvertragsklauseln

Maßnahme

Als Teil ihrer vertraglichen Auflagen sollten Angestellte, Auftragnehmer und Drittbenutzer den Vertragsklauseln ihres Anstellungsvertrags zustimmen und diesen unterzeichnen; diese Klauseln sollten ihre und die Verantwortlichkeiten der Organisation für Informationssicherheit festlegen.

Anleitung zur Umsetzung

Die Arbeitsvertragsklauseln sollten die Sicherheitsgrundsätze der Organisation widerspiegeln, und außerdem die folgenden Punkte verdeutlichen und feststellen:

- a) dass alle Angestellten, Auftragnehmer und Drittbenutzer, die Zugang zu sensiblen Informationen erhalten, eine Vertraulichkeits- oder Geheimhaltungsverpflichtung unterzeichnen sollten, bevor sie Zugang zu informationsverarbeitenden Einrichtungen erhalten;
- b) die gesetzlichen Verantwortlichkeiten und Rechte der Angestellten, Auftragnehmer und Drittbenutzer, z. B. bezüglich Urheberrecht oder Datenschutzgesetzgebung (siehe auch 15.1.1 und 15.1.2);
- c) Verantwortlichkeiten für die Klassifizierung von Informationen und das Management von organisationseigenen Werten, die zusammen mit Informationssystemen und Dienstleistungen von Angestellten, Auftragnehmer und Drittbenutzer betrieben werden (siehe auch 7.2.1 und 10.7.3);
- d) Verantwortlichkeiten der Angestellten, Auftragnehmer und Drittbenutzer für die Handhabung von Informationen, die von anderen Firmen oder Externen bereitgestellt wurden;
- e) Verantwortlichkeiten der Organisation für den Umgang mit personenbezogenen Daten, einschließlich der Daten, die als Ergebnis von oder im Laufe eines Arbeitsverhältnisses bei der Organisation erstellt wurden (siehe auch 15.1.4);
- f) Verantwortlichkeiten, die außerhalb des Geländes der Organisation und außerhalb der üblichen Arbeitszeit wirksam sind, z. B. bei Telearbeit von zuhause aus (siehe auch 9.2.5 und 11.7.1);
- g) Aktionen, die eingeleitet werden, wenn ein Angestellter, Auftragnehmer oder Drittbenutzer die Sicherheitsanforderungen der Organisation missachtet (siehe auch 8.2.3).

Die Organisation sollte sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer Vertragsklauseln für Informationssicherheit akzeptieren, die berücksichtigen, welchen Zugang sie zu den organisationseigenen Werten in Zusammenhang mit Informationssystemen und Dienstleistungen haben werden.

Gegebenenfalls sollten die Verantwortlichkeiten, die in den Vertragsklauseln definiert sind, für einen bestimmten Zeitraum nach Beendigung des Vertragsverhältnisses gültig bleiben (siehe auch 8.3).

Weitere Informationen

Verhaltensregeln dürfen benutzt werden, um die Verantwortlichkeiten von Angestellten, Auftragnehmern und Drittbenutzern zu regeln, zum Beispiel für Vertraulichkeit, Datenschutz, Ethik, richtige Benutzung der organisationseigenen Geräte und Einrichtungen, und akzeptierte Verfahren, die von der Organisation erwartet werden. Der Auftragnehmer oder Drittbenutzer darf einer externen Organisation angehören, die unter Umständen im Auftrag der Person unter Vertrag ihrerseits vertraglich eingebunden sein muss.

8.2 Während der Anstellung

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer die Informationssicherheitsbedrohungen und -bedenken sowie ihre Verantwortlichkeiten und Pflichten kennen, und dass sie entsprechend ausgestattet sind, die organisationseigene Sicherheitsleitlinie bei ihrer normalen Arbeit zu befolgen, und das Risiko von menschlichen Fehlern zu reduzieren.

Die Verantwortlichkeit des Managements sollte definiert werden, um sicherzustellen, dass Sicherheit während des gesamten Beschäftigungsverhältnisses einer Person zur Anwendung kommt.

Ein angemessenes Niveau bezüglich des Bewusstseins, der Ausbildung und Schulung in Sicherheitsverfahren und des korrekten Gebrauchs von informationsverarbeitenden Einrichtungen sollte allen Angestellten, Auftragnehmern und Drittbenutzern nahegebracht werden, um potentielle Sicherheitsrisiken zu minimieren. Für die Behandlung von Sicherheitsverstößen sollte ein formales Disziplinarverfahren eingerichtet werden.

8.2.1 Verantwortung des Managements

Maßnahme

Das Management sollte verlangen, dass Angestellte, Auftragnehmer und Drittbenutzer Sicherheit in Übereinstimmung mit den festgelegten Leitlinien und Verfahren der Organisation anwenden.

Anleitung zur Umsetzung

Die Verantwortlichkeiten des Managements sollten beinhalten, dass sichergestellt wird, dass Angestellte, Auftragnehmer und Drittbenutzer:

- a) zur Wahrnehmung ihrer Informationssicherheitsaufgaben und -verantwortlichkeiten richtig instruiert sind, bevor ihnen Zugang zu sensiblen Informationen oder Informationssystemen gegeben wird;
- b) mit Anweisungen ausgestattet werden, die die Erwartungen an Sicherheit für ihre Aufgabe in der Organisation darlegen;
- c) motiviert sind, die Sicherheitsleitlinie der Organisation zu erfüllen;
- d) einen Grad von Bewusstsein für Sicherheit erreichen, der entsprechend ihrer Aufgaben und Verantwortlichkeiten in der Organisation ist (siehe auch 8.2.2);
- e) ihren Arbeitsvertrag erfüllen, der die organisationseigene Informationssicherheitsleitlinie und entsprechende Arbeitspraktiken enthält;
- f) die erforderlichen Fähigkeiten und Qualifikationen haben und beibehalten.

Weitere Informationen

Wenn Angestellten, Auftragnehmern und Drittbenutzern ihre Sicherheitsverantwortlichkeiten nicht bewusst gemacht werden, können sie beträchtlichen Schaden für die Organisation verursachen. Motiviertes Personal ist im Allgemeinen viel verlässlicher, und verursacht weniger Informationssicherheitsvorfälle.

Schlechtes Management kann dazu führen, dass sich Angestellte unterschätzt fühlen, was negative Auswirkungen auf die Sicherheit der Organisation haben kann. Zum Beispiel kann schlechtes Management zur Vernachlässigung der Sicherheit oder zum Missbrauch von organisationseigenen Werten führen.

8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit

Maßnahme

Alle Angestellten der Organisation, und, falls relevant, Auftragnehmer und Drittbenutzer, sollten geeignete Sensibilisierungsmaßnahmen in Sachen Informationssicherheit erhalten, und regelmäßig über organisations-eigene Leitlinien und Verfahren, die für ihre Arbeit von Bedeutung sind, informiert werden.

Anleitung zur Umsetzung

Die Sensibilisierungsmaßnahmen zum Thema Informationssicherheit sollten mit einem formalen Einführungsprozess beginnen, um die Sicherheitsleitlinien und Erwartungen der Organisation vorzustellen, bevor Zugang zu Informationen oder Diensten gestattet wird.

Fortlaufende Schulungen sollten Sicherheitsanforderungen, gesetzliche Auflagen und Geschäftsmaßnahmen beinhalten, genauso wie Schulungen in der ordnungsgemäßen Nutzung von informationsverarbeitenden Einrichtungen, z. B. Verfahren zum Einloggen, Benutzung von Programmpaketen und Informationen über das Disziplinarverfahren (siehe 8.2.3);

Weitere Informationen

Die Aktivitäten zur Sensibilisierung, Ausbildung und Schulung sollten auf die Aufgaben, Verantwortlichkeiten und Fähigkeiten der Person ausgerichtet sein, und sollten Informationen über bekannte Bedrohungen, Kontakte für Beratung in Sicherheitsfragen und die geeigneten Kanäle für das Melden von Informationssicherheitsvorfällen (siehe auch 13.1) bereitstellen.

Sensibilisierungsmaßnahmen in Sachen Informationssicherheit sollten Personen in die Lage versetzen, Informationssicherheitsprobleme und -vorfälle zu erkennen und im Einklang mit den Erfordernissen ihres Aufgabengebiets zu reagieren.

8.2.3 Disziplinarverfahren

Maßnahme

Für Angestellte, die einen Sicherheitsverstoß begangen haben, sollte ein formales Disziplinarverfahren eingeleitet werden.

Anleitung zur Umsetzung

Das Disziplinarverfahren sollte erst begonnen werden nachdem geprüft werden konnte, dass ein Sicherheitsverstoß begangen wurde (siehe auch 13.2.3 für das Sammeln von Beweisen).

Das formale Disziplinarverfahren sollte eine korrekte, faire Behandlung der Angestellten gewährleisten, die im Verdacht stehen, Sicherheitsverstöße begangen zu haben. Das Disziplinarverfahren sollte eine abgestufte Reaktion ermöglichen, wobei Faktoren berücksichtigt werden wie die Art und Schwere des Verstoßes und seine Auswirkung auf das Geschäft, ob es ein erster oder wiederholter Verstoß ist, ob der Verursacher des Verstoßes angemessen geschult war oder nicht, ob entsprechende Gesetze oder Geschäftsverträge verletzt wurden, und gegebenenfalls andere Faktoren. Bei gravierenden Verstößen sollte der Prozess den sofortigen Entzug von Aufgaben, Zugangsrechten und Privilegien, und, wenn nötig, die unverzügliche Entfernung aus dem Gebäude vorsehen.

Weitere Informationen

Das Disziplinarverfahren sollte auch als Abschreckung für Angestellte, Auftragnehmer und Drittbenutzer dienen, die sonst Sicherheitsleitlinien und -verfahren der Organisation missachten könnten, oder andere Sicherheitsverstöße begehen.

8.3 Beendigung oder Änderung der Anstellung

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer ordnungsgemäß die Organisation verlassen, oder die Anstellung wechseln.

Verantwortlichkeiten sollten etabliert werden, um sicherzustellen, dass Angestellte, Auftragnehmer oder Drittbenutzer die Organisation in geregelter Weise verlassen, und dass die Rückgabe aller Geräte und das Entfernen der Zugangsrechte abgeschlossen sind.

Änderungen von Verantwortlichkeiten und Anstellungen innerhalb einer Organisation sollten genauso behandelt werden wie die Beendigung des jeweiligen Anstellungsverhältnisses oder der Verantwortlichkeiten, wie in diesem Abschnitt beschrieben, und jegliche Neuanstellungen sollten behandelt werden wie in 8.1 beschrieben.

8.3.1 Verantwortlichkeiten bei der Beendigung

Maßnahme

Die Verantwortlichkeiten für das Beenden oder Ändern eines Anstellungsverhältnisses sollten klar definiert und zugewiesen werden.

Anleitung zur Umsetzung

Die bei der Beendigung kommunizierten Verantwortlichkeiten sollten die aktuellen Sicherheitsanforderungen und gesetzliche Verantwortlichkeiten enthalten, und, falls passend, die in Vertraulichkeitsabkommen enthaltenen Verantwortlichkeiten (siehe 6.1.5), und die fortlaufende Gültigkeit der Arbeitsvertragsklauseln (siehe 8.1.3) für einen festgelegten Zeitraum nach der Beendigung der Anstellung des Angestellten, Auftragnehmers oder Drittbenutzers.

Verantwortlichkeiten und Pflichten, die nach der Beendigung der Anstellung noch gültig sind, sollten in den Verträgen mit den Angestellten, Auftragnehmern oder Drittbenutzern enthalten sein.

Änderungen von Verantwortung oder Anstellung sollten wie die Beendigung des jeweiligen Anstellungsverhältnisses oder der Verantwortung behandelt werden, und die neue Verantwortung oder Anstellung sollte wie in 8.1 beschrieben kontrolliert werden.

Weitere Informationen

Das Personalwesen ist normalerweise verantwortlich für den gesamten Beendigungsprozess und arbeitet zusammen mit dem beaufsichtigenden Manager der Person, die die Organisation verlässt, um die Sicherheitsaspekte der relevanten Verfahren zu handhaben. Im Fall eines Auftragnehmers darf der Beendigungsprozess von einer Agentur ausgeführt werden, und im Fall anderer Benutzer darf dies von deren Organisation übernommen werden.

Es kann notwendig sein, Angestellte, Kunden, Auftragnehmer oder Drittbenutzer über die Änderungen der Personal- und Betriebsprozesse zu informieren.

8.3.2 Rückgabe von organisationseigenen Werten

Maßnahme

Alle Angestellte, Auftragnehmer und Drittbenutzer sollten alle organisationseigenen Werte (Assets) in ihrem Besitz bei der Beendigung ihres Anstellungsverhältnisses, Vertrags oder Vereinbarung zurückgeben.

Anleitung zur Umsetzung

Der formale Beendigungsprozess sollte die Rückgabe aller vorher zugeteilten Software, organisationseigenen Dokumente und Geräte beinhalten. Andere organisationseigene Werte, wie mobile Computer, Kreditkarten, Zugangskarten, Softwarehandbücher und auf elektronischen Medien gespeicherte Informationen müssen ebenfalls zurückgegeben werden.

Falls ein Angestellte, Auftragnehmer oder Drittbenutzer organisationseigene Geräte kauft oder eigene, persönliche Geräte benutzt, sollten Verfahren befolgt werden, um sicherzustellen, dass alle relevanten Informationen an die Organisation übertragen werden und von den Geräten sicher gelöscht werden (siehe auch 10.7.1).

Falls ein Angestellter, Auftragnehmer oder Drittbenuer Kenntnis haben, die wichtig für laufende Operationen sind, so sollten diese Informationen dokumentiert und an die Organisation übertragen werden.

8.3.3 Zurücknahme von Zugangsrechten

Maßnahme

Die Zugangsrechte aller Angestellten, Auftragnehmer und Drittbenuer zu Informationen und informationsverarbeitenden Einrichtungen sollten zurückgenommen werden, wenn ihre Anstellung, Vertrag oder Vereinbarung endet, oder bei Veränderungen angepasst werden.

Anleitung zur Umsetzung

Bei Beendigung der Anstellung sollten die Zugangsrechte der Person zu Werten in Verbindung mit Informationssystemen und Dienstleistungen neu überdacht werden. Dies wird bestimmen, ob es nötig ist, die Zugangsrechte zu entziehen. Änderungen eines Anstellungsverhältnisses sollten sich in der Zurücknahme aller Zugangsrechte, die für die neue Anstellung nicht bestätigt wurden, widerspiegeln. Die Zugangsrechte, die zurückgenommen oder angepasst werden sollten, beinhalten physischen und logischen Zugang, Schlüssel, Identifikationskarten, informationsverarbeitende Einrichtungen (siehe auch 11.2.4), Abonnements, und das Entfernen von jeglichen Unterlagen, die die Person als momentanes Mitglied der Organisation ausweisen. Wenn ein ausscheidender Angestellter, Auftragnehmer oder Drittbenuer bekannte Passworte für Benutzerkonten hat, die aktiv bleiben, so sollten diese bei Beendigung oder Änderung der Anstellung, des Vertrags oder der Vereinbarung geändert werden.

Zugangsrechte für Informationswerte und informationsverarbeitende Einrichtungen sollten reduziert oder zurückgenommen werden bevor die Anstellung endet oder sich ändert; dies sollte abhängig von der Bewertung von Risikofaktoren sein, wie zum Beispiel:

- a) ob die Beendigung oder Änderung von dem Angestellten, Auftragnehmer oder Drittbenuer eingeleitet wurde, oder durch das Management, und der Grund für die Beendigung;
- b) die momentanen Verantwortlichkeiten des Angestellten, Auftragnehmers oder anderen Benutzers;
- c) der Wert der momentan zugänglichen organisationseigenen Werte (Assets).

Weitere Informationen

Unter bestimmten Umständen dürfen die Zugangsrechte auf der Basis vergeben werden, dass sie für mehrere Personen als den ausscheidenden Angestellten, Auftragnehmer oder Drittbenuer bereitgestellt werden, z. B. Gruppen-IDs. Unter diesen Umständen sollte die ausscheidende Person von allen Gruppenzugangslisten entfernt werden, und Vorkehrungen sollten getroffen werden, um alle anderen betroffenen Angestellten, Auftragnehmer oder Drittbenuer zu unterrichten, dass sie die Informationen mit der ausscheidenden Person nicht länger teilen sollten.

Falls die Beendigung vom Management veranlasst wurde, könnten verärgerte Angestellte, Auftragnehmer oder Drittbenuer absichtlich Informationen beschädigen oder informationsverarbeitende Einrichtungen sabotieren. Falls Personen kündigen, könnten sie versucht sein, Informationen für ihren zukünftigen persönlichen Gebrauch zu sammeln.

9 Physische und umgebungsbezogene Sicherheit

9.1 Sicherheitsbereiche

Ziel: Schutz vor unerlaubtem Zutritt zu und Beschädigung und Störung von Organisationsinfrastruktur und der Organisation gehörenden Informationen.

Kritische oder sensitive datenverarbeitende Einrichtungen sollten in Sicherheitsbereichen untergebracht sein, welche durch festgelegte Sicherheitszonen mit angemessenen Sicherheitsbarrieren und Zugangskontrollsystemen geschützt sind.

Diese Maßnahmen sollten im Einklang mit den identifizierten Risiken stehen.

9.1.1 Sicherheitszonen

Maßnahme

Sicherheitszonen (Hindernisse wie Wände, über Zutrittskarten kontrollierte Zugänge oder mit Pförtnern besetzte Empfangsbereiche) sollten die Abschnitte schützen, die informationsverarbeitende Einrichtungen beherbergen.

Anleitung zur Umsetzung

Die folgende Anleitung sollte berücksichtigt und wo angemessen, für Sicherheitsbereiche umgesetzt werden.

- a) Sicherheitszonen sollten klar festgelegt sein. Die Lage und die Stärke einer jeden Sicherheitszone sollten den durch die Risikobetrachtung ermittelten Sicherheitsanforderungen der in der Zone befindlichen organisationseigenen Werte (Assets) entsprechen.
- b) Die Begrenzungen eines Gebäudes oder eines Standorts, das informationsverarbeitende Einrichtungen beherbergt, sollten physisch solide sein (d. h. es gibt keine Löcher in der Grenzeinfassung (Zaun, Mauer) die einen Einbruch stark vereinfachen). Die äußeren Wände eines Standorts sollten stabil konstruiert (aus Vollmauerwerk/Beton) sein. Alle Türen nach außen sollten einen angemessenen Schutz gegen unautorisierten Zugang bieten, z. B. Gitter, Alarmierung, Schlösser usw. Türen und Fenster sollten verschlossen sein, wenn keine Personen der Organisation anwesend sind. Zusätzlicher Schutz für Fenster, insbesondere im Erdgeschoss (z. B. Vergitterung) sollte in Betracht gezogen werden.
- c) Ein Pförtner oder andere Einrichtungen zur Zutrittskontrolle sollten für ein solches Gebäude oder einen Standort vorhanden sein. Der Zugang sollte sich auf autorisierte Mitarbeiter beschränken.
- d) Physische Barrieren sollten, wo angemessen, unautorisierten Zutritt und Verschmutzung durch die Umgebung verhindern.
- e) Alle Brandschutztüren einer Sicherheitszone sollten alarmgesichert, überwacht und in Verbindung mit den anschließenden Wänden getestet werden, um so das notwendige Maß hinsichtlich des Brandschutzes sicherzustellen. Dies sollte in Einklang mit regionalen, nationalen und internationalen Standards geschehen. Diese Komponenten sollten, gemäß den lokalen Brandschutzbestimmungen, störungssicher funktionieren.
- f) Angemessene, den nationalen, regionalen oder internationalen Standards entsprechende Einbruchmeldesysteme, die alle Außentüren und von außen erreichbaren Fenster überwachen, sollten vorhanden sein und regelmäßig getestet werden. Räumlichkeiten, die nicht von Mitarbeitern besetzt sind, sollten einer permanenten Überwachung unterliegen, gleiches gilt für Computer- und Kommunikationsräume.
- g) Durch die Organisation verwaltete, informationsverarbeitende Einrichtungen sollten physisch von informationsverarbeitenden Einrichtungen getrennt sein, die durch Externe administriert oder betrieben werden.

Weitere Informationen

Physischer Schutz kann durch eine oder mehrere physische Hindernisse um einen Organisationsstandort und dessen informationsverarbeitenden Einrichtungen erreicht werden. Die Verwendung von mehreren Hindernissen bietet zusätzlichen Schutz, da das Versagen eines einzelnen Hindernisses nicht automatisch bedeutet, dass die Sicherheit kompromittiert wurde.

Ein Sicherheitsbereich darf ein abschließbares Büro oder mehrere Räume, die innerhalb eines physikalisch abgegrenzten Bereichs liegen, sein. Zusätzliche Abgrenzungen und Barrieren zur Zutrittskontrolle können dort notwendig werden, wo es unterschiedliche Sicherheitsanforderungen zwischen den Bereichen gibt.

Besondere Aufmerksamkeit ist im Hinblick auf Zutrittskontrolle dort notwendig, wo sich mehrere Organisationen einen Standort teilen.

9.1.2 Zutrittskontrolle

Maßnahme

Sicherheitsbereiche sollten durch angemessene Zutrittskontrollen geschützt sein, um sicherzustellen, dass nur autorisierten Mitarbeitern Zutritt gewährt wird.

Anleitung zur Umsetzung

Die folgenden Regelungen sollten in Betracht gezogen werden:

- a) Datum und Uhrzeit des Zutritts und des Verlassens eines Bereiches durch einen Besucher sollten aufgezeichnet werden. Alle Besucher sollten permanent überwacht/begleitet werden, es sei denn, ihr Zugang ist vorher entsprechend autorisiert worden; Besucher sollten nur Zugang zu festgelegten, autorisierten Zwecken haben, sie sollten von den Sicherheitsanforderungen des Bereiches sowie über das Verhalten im Notfall in Kenntnis gesetzt worden sein;
- b) Zugang zu Bereichen in denen sensitive Informationen verarbeitet oder gespeichert werden, sollte kontrolliert werden und nur autorisierten Personen gewährt werden; Maßnahmen zur Authentisierung, z. B. Chipkarten mit PIN für den Zutritt, sollten für die Autorisierung des Zugangs herangezogen werden. Die Nachvollziehbarkeit aller Zutrittsvorgänge muss sichergestellt sein;
- c) alle Mitarbeiter, Vertragspartner und Dritte sowie alle Besucher sollten eine sichtbare Identifikation tragen. Das Sicherheitspersonal sollte unverzüglich informiert werden, wenn Fremde ohne Begleitung oder Personen, die keine sichtbare Identifikation tragen bemerkt werden;
- d) Dienstleister und Dritte sollten nur dann Zutritt zu Sicherheitszonen oder informationsverarbeitenden Einrichtungen mit sensitiven Daten erhalten, wenn dies erforderlich ist. Dieser Zutritt sollte autorisiert und überwacht werden;
- e) Zutrittsrechte zu Sicherheitszonen sollten regelmäßig überprüft, aktualisiert und wenn notwendig entzogen werden (siehe 8.3.3).

9.1.3 Sicherung von Büros, Räumen und EinrichtungenMaßnahme

Physischer Schutz für Büros, Räume und Einrichtungen sollte geplant und umgesetzt werden.

Anleitung zur Umsetzung

Die folgenden Regelungen sollten berücksichtigt werden, um Büros, Räume und Einrichtungen zu sichern:

- a) die Einhaltung relevanter Gesundheits- und Sicherheitsvorschriften soll sichergestellt werden;
- b) wichtige Einrichtungen sollten so gelegen sein, dass sie der Allgemeinheit nicht zugänglich sind;
- c) Gebäude sollten so unauffällig wie möglich sein und möglichst keine Hinweise auf ihren Zweck bereitstellen. Es sollten keine Zeichen und Schilder, weder außen noch innen, einen Hinweis auf informationsverarbeitende Aktivitäten geben;
- d) Verzeichnisse und interne Telefonbücher, die einen Hinweis auf die Lage von informationsverarbeitenden Einrichtungen mit sensitiven Informationen geben, sollten nicht öffentlich zugänglich sein.

9.1.4 Schutz vor Bedrohungen von außen und aus der UmgebungMaßnahme

Physischer Schutz gegen Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und andere Formen natürlicher und von Menschen verursachter Katastrophen sollte vorgesehen und umgesetzt sein.

Anleitung zur Umsetzung

Potentielle Bedrohungen aus der Umgebung sollten auch in Betracht gezogen werden, z. B. ein Feuer in einem Nachbargebäude, Wasserschäden durch ein undichtes Dach oder Rohrbrüche im Kellergeschoss oder eine Explosion auf der Straße.

Die folgenden Regelungen sollten in Betracht gezogen werden, um Schäden durch Feuer, Flut, Erdbeben, Explosionen, zivile Unruhen und anderen Formen natürlicher und von Menschen verursachter Katastrophen zu vermeiden:

- a) gefährliche und leicht entzündliche Materialien sollten in sicherer Entfernung von Sicherheitszonen gelagert werden. Materialien mit hoher Brandlast, wie Schreibmaterial und Papier, sollten generell nicht in einer Sicherheitszone gelagert werden;
- b) Ersatzgeräte und Backup-Medien sollten in sicherer Entfernung von der Sicherheitszone untergebracht sein um zu verhindern, dass diese bei einem Schaden am primären Standort auch betroffen sind;
- c) angemessene Ausstattung zur Brandbekämpfung sollte bereitgestellt und adäquat platziert sein.

9.1.5 Arbeiten in Sicherheitszonen

Maßnahme

Physischer Schutz und Richtlinien für die Arbeit in Sicherheitszonen sollten entwickelt und umgesetzt werden.

Anleitung zur Umsetzung

Die folgenden Regelungen sollten berücksichtigt werden:

- a) das Personal sollte nur bei Bedarf (Need-to-know-Basis) von der Existenz einer Sicherheitszone und den Aktivitäten innerhalb der Zone Kenntnis haben;
- b) nichtüberwachtes Arbeiten in Sicherheitszonen sollte, aus Gründen der Sicherheit und um Gelegenheiten für schädliche Aktivitäten (Sabotage) zur verringern, vermieden werden;
- c) nichtbesetzte Sicherheitszonen sollten verschlossen und regelmäßig kontrolliert werden;
- d) das Mitführen von Aufnahmegeräten gleich welcher Art sollte, sofern nicht explizit gestattet, verboten sein.

Die Vereinbarungen für das Arbeiten in Sicherheitszonen enthalten Maßnahmen für Mitarbeiter, Vertragspartner und Dienstleister, die in Sicherheitszonen arbeiten, genauso wie für sonstige Aktivitäten Dritter, die dort erfolgen.

9.1.6 Öffentlicher Zugang, Anlieferungs- und Ladezonen

Maßnahme

Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Zugangspunkte, an denen unbefugte Personen den Standort betreten können, sollten kontrolliert und, sofern möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unerlaubten Zutritt zu verhindern.

Anleitung zur Umsetzung

Die folgenden Regelungen für Zugangskontrollen sollten berücksichtigt werden:

- a) Zugang zur Anlieferungs- und Ladezone eines Gebäudes von außerhalb sollte nur identifiziertem und berechtigtem Personal erlaubt sein;
- b) die Anlieferungs- und Ladezone sollte so gestaltet sein, dass Lieferungen ausgeladen werden können, ohne dass das Lieferpersonal Zutritt zu anderen Bereichen des Gebäudes erhält;
- c) die Außentüren einer Anlieferungs- und Ladezone sollten gesichert sein, wenn die Türen zum inneren Bereich geöffnet sind;
- d) eingehendes Material sollte auf potentielle Bedrohungen hin untersucht werden (siehe 9.2.1d)) bevor dieses Material aus der Anlieferungs- und Ladezone zu seinem Bestimmungsort gebracht wird;
- e) eingehendes Material sollte bei Anlieferung laut Vorgaben inventarisiert werden (siehe auch 7.1.1);