

DIN ISO/IEC 27002

ICS 35.040

Einsprüche bis 2014-03-10
Vorgesehen als Ersatz für
DIN ISO/IEC 27002:2008-09

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Leitfaden für das Informationssicherheits-Management
(ISO/IEC FDIS 27002:2013)**

Information technology –
Security techniques –
Code of practice for information security management (ISO/IEC FDIS 27002:2013)

Technologies de l'information –
Techniques de sécurité –
Code de bonne pratique pour le management de la sécurité de l'information
(ISO/CEI FDIS 27002:2013)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-01-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 103 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Inhalt

	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
0 Einleitung	6
0.1 Hintergrund und Zusammenhänge	6
0.2 Anforderungen an Informationssicherheit	7
0.3 Auswahl von Sicherheitsmaßnahmen	7
0.4 Entwicklung eigener Richtlinien	7
0.5 Berücksichtigung von Lebenszyklen	8
0.6 Zugehörige Normen	8
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Aufbau dieser Norm	9
4.1 Abschnitte	9
4.2 Kategorien von Sicherheitsmaßnahmen	10
5 Sicherheitsleitlinien	10
5.1 Managementausrichtung zur Informationssicherheit	10
6 Organisation der Informationssicherheit	12
6.1 Interne Organisation	12
6.2 Mobilgeräte und Telearbeit	15
7 Personalsicherheit	18
7.1 Vor der Anstellung	18
7.2 Während der Anstellung	20
7.3 Beendigung und Wechsel der Anstellung	22
8 Management von organisationseigenen Werten	23
8.1 Verantwortung für organisationseigene Werte	23
8.2 Klassifizierung von Informationen	25
8.3 Handhabung von Speicher- und Aufzeichnungsmedien	28
9 Zugriffskontrolle	30
9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle	30
9.2 Benutzerverwaltung	32
9.3 Benutzerverantwortung	37
9.4 Kontrolle des Zugangs zu Systemen und Anwendungen	38
10 Kryptographie	42
10.1 Kryptographische Maßnahmen	42
11 Schutz vor physischem Zugang und Umwelteinflüssen	44
11.1 Sicherheitsbereiche	44
11.2 Sicherheit von Betriebsmitteln	48
12 Betriebssicherheit	54
12.1 Betriebsverfahren und Zuständigkeiten	54
12.2 Schutz vor Malware	57
12.3 Backup	59
12.4 Protokollierung und Überwachung	60
12.5 Kontrolle von Betriebssoftware	62

12.6	Technisches Schwachstellenmanagement	64
12.7	Auswirkungen von Audits auf Informationssysteme	66
13	Sicherheit in der Kommunikation	67
13.1	Netzwerksicherheitsmanagement	67
13.2	Informationsübertragung	69
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	73
14.1	Sicherheitsanforderungen für Informationssysteme	73
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	76
14.3	Prüfdaten	82
15	Lieferantenbeziehungen	82
15.1	Informationssicherheit bei Lieferantenbeziehungen	82
15.2	Management der Dienstleistungserbringung durch Lieferanten	86
16	Management von Informationssicherheitsvorfällen	88
16.1	Management von Informationssicherheitsvorfällen und Verbesserungen	88
17	Informationssicherheitsaspekte des Betriebskontinuitätsmanagements	93
17.1	Aufrechterhaltung der Informationssicherheit	93
17.2	Redundanzen	95
18	Richtlinienkonformität	96
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	96
18.2	Informationssicherheitsprüfungen	99
	Literaturhinweise	102

Nationales Vorwort

Die Internationale Norm ISO/IEC FDIS 27002:2013-05 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.

Änderungen

Gegenüber DIN ISO/IEC 27002:2008-09 wurden folgende Änderungen vorgenommen:

- a) Anpassung an die neue Struktur für ISO Management System Standards, vorgegeben im Annex SL der ISO/IEC Direktiven.
- b) Die Norm wurde redaktionell überarbeitet.

Für die in diesem Dokument zitierte internationale Norm wird im folgenden auf die entsprechende deutsche Norm hingewiesen:

ISO/IEC 27000 siehe DIN ISO/IEC 27000

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-
Managementsysteme — Überblick und Terminologie*

Informationstechnologie — Sicherheitsverfahren — Leitfaden für Maßnahmen zur Informationssicherheit

0 Einleitung

0.1 Hintergrund und Zusammenhänge

Diese Internationale Norm wurde erarbeitet, um Organisationen als Referenz zur Auswahl von Maßnahmen bei der Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001 zu dienen oder als Leitfaden für Organisationen, die gemeinhin akzeptierte Maßnahmen für die Informationssicherheit einführen möchten. Dieser Standard ist ebenfalls bestimmt für die Entwicklung von branchen- und organisationsspezifischen Leitfäden zum Management von Informationssicherheit. Dabei wird das Umfeld der spezifischen Informationssicherheitsrisiken berücksichtigt.

Organisationen aller Arten und Größen (einschließlich öffentlicher und privater, kommerzieller und gemeinnütziger) erheben, verarbeiten, speichern und übertragen Informationen in vielen Formen, darunter elektronisch, physisch und verbal (z. B. Gespräche und Präsentationen).

Der Informationswert besteht nicht nur aus geschriebenen Wörtern, Zahlen und Bildern: Wissen, Konzepte, Ideen und Marken sind Beispiele für immaterielle Informationsformen. Informationen und damit verbundene Prozesse, Systeme, Netzwerke und Personal zu deren Verarbeitung, Handhabung und Schutz stellen in einer vernetzten Welt organisationseigene Werte dar, die genauso wie andere wichtige Unternehmensressourcen für die Geschäftsziele einer Organisation wichtig sind, und damit einen Schutz gegen unterschiedliche Gefährdungen verdienen oder erfordern.

Organisationseigene Werte unterliegen sowohl vorsätzlichen als auch versehentlichen Bedrohungen, während damit verbundene Prozesse, Systeme, Netzwerke und Menschen ihre innewohnenden Schwächen zeigen. Änderungen von Geschäftsprozessen und Unternehmenssystemen oder andere externe Veränderungen (z. B. neue Gesetze und Verordnungen) können zu neuen Risiken in der Informationssicherheit führen. Angesichts der vielfältigen, potenziellen Bedrohungen, die Schwachstellen zum Schaden der Organisation ausnutzen, bestehen daher immer Risiken in der Informationssicherheit. Eine wirkungsvolle Informationssicherheit verringert diese Risiken durch Schutz der Organisation vor Bedrohungen und Schwachstellen und vermindert dadurch die Auswirkungen auf organisationseigene Werte.

Die Einführung einer Reihe geeigneter Sicherheitsmaßnahmen, darunter Richtlinien, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen, sorgt für Informationssicherheit. Zur Erfüllung spezifischer Sicherheits- und Geschäftsziele der Organisation müssen diese Sicherheitsmaßnahmen eingeführt, verwirklicht, überwacht, überprüft und gegebenenfalls verbessert werden. Ein Informationssicherheits-Managementsystem (ISMS), wie in ISO/IEC 27001 näher beschrieben, verfolgt eine ganzheitliche, koordinierte Betrachtung der Risiken in der Informationssicherheit eines Unternehmens, um eine umfassende Suite von Maßnahmen zur Informationssicherheit im Rahmen eines einheitlichen Managementsystems einführen zu können.

Viele Informationssysteme sind nicht so konzipiert, dass sie im Sinne von ISO/IEC 27001 und dieser Norm als sicher betrachtet werden können. Die Sicherheit mithilfe technischer Mittel ist begrenzt und sollte mit geeigneten Verwaltungsmitteln und Verfahren unterstützt werden. Die Feststellung der benötigten Sicherheitsmaßnahmen erfordert sorgfältige Planung und Detailtreue. Ein erfolgreiches Informationssicherheits-Managementsystem erfordert die Mitarbeit aller Mitarbeiter einer Organisation. Die Organisation benötigt unter Umständen auch die Mitwirkung von Gesellschaftern, Lieferanten und anderen externen Stellen. Fachliche Beratung durch externe Stellen könnte ebenfalls benötigt werden.

Eine wirkungsvolle Informationssicherheit gibt im Allgemeinen auch dem Management und anderen Beteiligten die Gewissheit, dass organisationseigene Werte einigermaßen sicher und gegen Schaden geschützt sind: Informationssicherheit wird so zum Geschäftserfordernis.

0.2 Anforderungen an Informationssicherheit

Es ist wichtig, dass eine Organisation ihre Sicherheitsanforderungen ermittelt. Die drei hauptsächlichen Beweggründe für Sicherheitsanforderungen:

- a) Bewertung der Risiken für die Organisation unter Berücksichtigung der Unternehmensstrategie und des Geschäftszwecks. Mithilfe einer Risikobewertung können Bedrohungen der organisationseigenen Werte ermittelt, Anfälligkeit und Eintrittswahrscheinlichkeit bewertet und mögliche Auswirkungen geschätzt werden;
- b) rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen, die eine Organisation, seine Handelspartner, Auftragnehmer und Dienstleister erfüllen müssen sowie deren soziokulturelles Umfeld;
- c) eine Reihe von Grundsätzen, Zielsetzungen und Geschäftserfordernissen, die eine Organisation für den Umgang mit Information sowie deren Verarbeitung, Speicherung, Kommunikation und Archivierung in Unterstützung ihrer Geschäftstätigkeit entwickelt hat.

Ressourcen zur Einführung von Sicherheitsmaßnahmen müssen gegen den Unternehmensschaden abgewogen werden, der wahrscheinlich bei Fehlen dieser Maßnahmen durch Sicherheitsprobleme verursacht wird. Die Ergebnisse einer Risikobewertung werden dabei helfen, geeignete betriebliche Maßnahmen und Prioritäten zur Bewältigung von Risiken der Informationssicherheit festzusetzen und zu betreuen und ausgewählte Sicherheitsmaßnahmen zum Schutz gegen diese Risiken einzuführen.

ISO/IEC 27005 bietet eine Anleitung zum Management von Informationssicherheitsrisiken, einschließlich Empfehlungen zu Bewertung, Behandlung, Akzeptanz, Kommunikation, Überwachung und Prüfung von Risiken.

0.3 Auswahl von Sicherheitsmaßnahmen

Sicherheitsmaßnahmen können entweder dieser Norm oder einer anderen Reihe entnommen werden. Auch neue Sicherheitsmaßnahmen können entwickelt werden, um gegebenenfalls spezifische Anforderungen zu erfüllen.

Die Auswahl der Sicherheitsmaßnahmen ist abhängig von organisatorischen Entscheidungen, denen die Kriterien für Risikoakzeptanz, Risikobehandlungsmöglichkeiten und die allgemeine Haltung der Organisation bezüglich des Risikomanagements zugrunde liegen. Die Auswahl sollte ebenfalls alle relevanten nationalen und internationalen Gesetze und Vorschriften berücksichtigen. Die Auswahl der Sicherheitsmaßnahmen hängt ebenfalls von der Art und Weise ab, wie Sicherheitsmaßnahmen interagieren, um gestaffelte Sicherheitsebenen bereitstellen zu können.

Einige der Sicherheitsmaßnahmen in dieser Norm können als Leitsätze zum Management für Informationssicherheit betrachtet werden und sind in den meisten Organisationen anwendbar. Die Sicherheitsmaßnahmen werden im Folgenden zusammen mit Umsetzungshinweisen näher erläutert. Weitere Informationen zur Auswahl von Sicherheitsmaßnahmen und anderen Risikobehandlungsmöglichkeiten sind in ISO/IEC 27005 verfügbar.

0.4 Entwicklung eigener Richtlinien

Diese Internationale Norm kann als Ausgangspunkt für die Entwicklung organisationsspezifischer Leitlinien angesehen werden. Möglicherweise sind nicht alle der in diesem Leitfaden angegebenen Sicherheitsmaßnahmen und Orientierungshilfen anwendbar. Darüber hinaus könnten zusätzliche, nicht hier aufgeführte Sicherheitsmaßnahmen und Richtlinien erforderlich sein. Bei der Verfassung von Dokumenten mit zusätzlichen Richtlinien oder Sicherheitsmaßnahmen kann es sinnvoll sein, gegebenenfalls Querverweise auf Abschnitte in dieser Norm anzugeben, um Konformitätsprüfungen durch Wirtschaftsprüfer und Geschäftspartner zu erleichtern.

0.5 Berücksichtigung von Lebenszyklen

Informationen haben einen natürlichen Lebenszyklus, von Erstellung und Entstehung über Speicherung, Verarbeitung, Verwendung und Weitergabe bis letztlich zu Zerstörung oder Verfall. Im Laufe ihres Lebenszyklus können organisationseigene Werte und damit verbundenen Risiken variieren (z. B. unberechtigte Weitergabe oder Diebstahl des Geschäftsberichts eines Unternehmens ist weit weniger bedeutsam, nachdem die Daten veröffentlicht wurden). In gewissem Maß ist Informationssicherheit jedoch in allen Phasen von Wichtigkeit.

Informationssysteme unterliegen Lebenszyklen, in denen sie konzipiert, festgelegt, entworfen, entwickelt, getestet, implementiert, genutzt, gepflegt und schließlich ausgemustert und vernichtet werden. Informationssicherheit sollte in jeder Phase berücksichtigt werden. Neue Systementwicklungen und Änderungen bestehender Systeme bieten Organisationen die Möglichkeit, ihre Sicherheitsmaßnahmen unter Berücksichtigung aktueller Vorfälle und projizierter Informationssicherheitsrisiken zu aktualisieren und zu verbessern.

0.6 Zugehörige Normen

Während dieser Standard als Orientierungshilfe für ein breites Spektrum an Maßnahmen für Informationssicherheit anzusehen ist, die üblicherweise in vielen Organisationen angewendet werden, bieten die übrigen Teile der ISO/IEC 27000 Normenfamilie ergänzende Empfehlungen oder zeigen Anforderungen bezüglich anderer Aspekte des Gesamtprozesses zum Management von Informationssicherheit.

ISO/IEC 27000 gibt eine allgemeine Einführung zu Informationssicherheitsmanagementsystemen und der Normenfamilie. ISO/IEC 27000 enthält ein Glossar für offizielle Definitionen der meisten Begriffe, die in der ISO/IEC 27000 Normenfamilie verwendet werden, und beschreibt Umfang und Zielsetzungen einzelnen Normen.

1 Anwendungsbereich

Diese Internationale Norm enthält Richtlinien für organisatorische Normen und Managementpraktiken bezüglich Informationssicherheit, einschließlich Auswahl, Implementierung und Management von Sicherheitsmaßnahmen unter Berücksichtigung des Umfelds der Informationssicherheitsrisiken in einer Organisation.

Diese Internationale Norm wurde für Organisationen entwickelt, die beabsichtigen:

- a) Maßnahmen für den Umsetzungsprozess eines Managementsystems für Informationssicherheit auf der Basis von ISO/IEC 27001 zu ergreifen,
- b) allgemein akzeptierte Maßnahmen für Informationssicherheit zu ergreifen,
- c) ihre eigenen Richtlinien eines Managements für Informationssicherheit zu entwickeln.

2 Normative Verweisungen

Das folgende zitierte Dokument ist für die Anwendung dieses Dokuments unverzichtbar. Bei datierten Verweisen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO/IEC 27000 angegebenen Begriffe.

4 Aufbau dieser Norm

Diese Norm enthält 14 Abschnitte über Sicherheitsmaßnahmen mit 35 Hauptkategorien der Sicherheit und 113 Sicherheitsmaßnahmen.

4.1 Abschnitte

Jeder Abschnitt, der Sicherheitsmaßnahmen definiert, enthält mindestens eine primäre Sicherheitskategorie.

Die Reihenfolge der Abschnitte lässt keinen Rückschluss auf ihre Bedeutung zu. Je nach Umstand können Sicherheitsmaßnahmen aus einer oder mehreren Kategorien wichtig sein. Daher sollte jede Organisation, die diese Norm anwenden möchte, für sie zutreffende Sicherheitsmaßnahmen identifizieren und feststellen, wie wichtig sie sind und inwieweit sie auf einzelne Geschäftsprozesse anwendbar sind. Darüber hinaus sind Listen in dieser Norm nicht Reihenfolge ihrer Priorität geordnet.

4.2 Kategorien von Sicherheitsmaßnahmen

Jede Hauptkategorie von Sicherheitsmaßnahmen enthält:

- a) Zielsetzung einer Sicherheitsmaßnahme und was erreicht werden soll;
- b) eine oder mehrere Sicherheitsmaßnahme(n), die zur Erreichung der Zielsetzung angewendet werden können.

Die Beschreibungen der Sicherheitsmaßnahmen sind wie folgt strukturiert:

Maßnahme

Definition der spezifischen Sicherheitsmaßnahme und Erklärung, wie das Ziel der Maßnahme erreicht wird.

Umsetzungshinweise

Bietet detaillierte Information zur Umsetzung von Sicherheitsmaßnahmen und um ihre Ziele zu erreichen. Die Hinweise sind vielleicht nicht in allen Situationen ausreichend oder könnten nur eingeschränkt anwendbar sein und erfüllen möglicherweise nicht die spezifische Sicherheitsanforderung einer Organisation.

Weitere Informationen

Enthält weitere zu berücksichtigende Informationen, wie rechtliche Aspekte und Verweise auf andere Normen. Falls keine weiteren Informationen zur Verfügung stehen, entfällt dieser Punkt.

5 Sicherheitsleitlinien

5.1 Managementausrichtung zur Informationssicherheit

Zielsetzung: Bereitstellung von Vorgaben und Unterstützung in Informationssicherheit seitens des Managements nach geschäftlichen Anforderungen und den geltenden Gesetzen und Vorschriften.

5.1.1 Informationssicherheitsleitlinien

Maßnahme

Eine Reihe von Leitlinien zur Informationssicherheit sollte definiert, vom Management genehmigt, bekannt gegeben und Mitarbeitern sowie relevanten externen Stellen mitgeteilt werden.

Umsetzungshinweise

Organisationen sollten auf höchster Ebene eine Leitlinie zur Informationssicherheit definieren, die vom Management genehmigt ist und einen Ansatz zur Bewältigung der Informationssicherheitsziele festlegt.

Leitlinien zur Informationssicherheit sollten Anforderungen ansprechen, die entstehen durch:

- a) eine Unternehmensstrategie;
- b) Vorschriften, Gesetze und Verträge;
- c) das aktuelle und voraussichtliche Umfeld von Bedrohungen der Informationssicherheit.

Die Leitlinie zur Informationssicherheit sollte Aussagen enthalten über:

- a) Die Definition von Informationssicherheit, Zielen und Grundsätzen, um alle Maßnahmen in Bezug auf Informationssicherheit lenken zu können;
- b) Zuordnung allgemeiner und spezifischer Verantwortlichkeiten für das Management von Informationssicherheit auf definierte Funktionen;
- c) Prozesse für den Umgang mit Abweichungen und Ausnahmen.

Auf niedrigeren Ebenen sollten die Leitlinien zur Informationssicherheit durch themenspezifische Richtlinien unterstützt werden, die zusätzlich eine Umsetzung von Maßnahmen zur Informationssicherheit erfordern. Diese Maßnahmen sind in der Regel so aufgebaut, dass die Bedürfnisse gewisser Zielgruppen einer Organisation angesprochen oder bestimmte Themen abgedeckt werden.

Beispiele für solche themenspezifische Richtlinien sind unter anderen:

- a) Zugangskontrolle (siehe 9);
- b) Klassifizierung von Information (und deren Behandlung) (siehe 8.2);
- c) Physische und umgebungsbezogene Sicherheit (siehe 11);
- d) an den Endanwender gerichtete Themen wie:
 - 1) zulässiger Gebrauch von organisationseigenen Werten (siehe 8.1.3);
 - 2) Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms (siehe 11.2.9);
 - 3) Austausch von Informationen (siehe 13.2.1);
 - 4) Mobilgeräte und Telearbeit (siehe 6.2);
 - 5) Einschränkungen für Softwareinstallation und -verwendung (siehe 12.6.2);
- e) Backup (siehe 12.3);
- f) Austausch von Informationen (siehe 13.2);
- g) Schutz vor Schadsoftware (siehe 12.2);
- h) Management technischer Schwachstellen (siehe 12.6.1);
- i) Kryptographische Maßnahmen (siehe 10);
- j) Sicherheit in der Kommunikation (siehe 13);
- k) Datenschutz und Vertraulichkeit von personenbezogenen Informationen (siehe 18.1.4);
- l) Lieferantenbeziehungen (siehe 15).

Diese Leitlinien sollten Mitarbeitern und allen maßgeblichen externen Stellen in einer Form mitgeteilt werden, die für die Zielgruppe relevant, zugänglich und verständlich ist, z. B. im Rahmen eines „Schulungsprogramms zur Sensibilisierung für Informationssicherheit“ (siehe 7.2.2).

Weitere Informationen

Der Bedarf an internen Leitlinien zur Informationssicherheit variiert je nach Organisation. Interne Leitlinien sind besonders nützlich in größeren, komplexeren Organisationen, in denen die Stellen, die zu erwartende Maßnahmenstufen festlegen und genehmigen, von den Stellen getrennt sind, die diese Maßnahmen einführen, oder wo eine Leitlinie für viele Mitarbeiter oder Funktionen einer Organisation gilt. Leitlinien zur Informationssicherheit können in einem einzelnen Dokument "Leitlinie zur Informationssicherheit" oder in mehreren einzelnen, aber zusammengehörigen Dokumenten verfasst werden.

Falls Leitlinien zur Informationssicherheit außerhalb der Organisation verbreitet werden, sollte darauf geachtet werden, dass keine vertraulichen Informationen mitgeteilt werden.

Einige Organisation verwenden Ausdrücke wie „Normen“, „Richtlinien“ oder „Regeln“ für diese Leitlinien.

5.1.2 Überprüfung der Informationssicherheitsleitlinien

Maßnahme

Die Informationssicherheitsleitlinien sollten in planmäßigen Abständen oder nach erheblichen Änderungen geprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

Umsetzungshinweise

Jede Leitlinie sollte einen Hauptverantwortlichen haben, der von Management autorisiert ist, Leitlinien zu entwickeln, zu überprüfen und zu bewerten. Die Überprüfung sollte eine Bewertung des Verbesserungspotenzials für Leitlinien und Methoden des Managements von Informationssicherheit in einer Organisation umfassen, als Antwort auf Änderungen im organisatorischen Umfeld, der geschäftlichen und gesetzlichen Rahmenbedingungen und der technischen Umgebung.

Die Überprüfung der Leitlinien zur Informationssicherheit sollte die Ergebnisse der Prüfungen durch Management enthalten.

Eine überarbeitete Leitlinie sollte durch das Management genehmigt werden.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Zielsetzung: Einführung eines Steuerungsrahmens, um Umsetzung und Einsatz von Informationssicherheit innerhalb einer Organisation anzubahnen und zu steuern.

6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit

Maßnahme

Alle Zuständigkeiten im Bereich der Informationssicherheit sollten festgelegt und zugeordnet werden.

Umsetzungshinweise

Verantwortlichkeiten für Informationssicherheit sollten in Übereinstimmung mit den Leitlinien zur Informationssicherheit zugeordnet werden (siehe 5.1.1). Verantwortungen zum Schutz individueller organisationseigener Werte und zur Anwendung spezifischer Prozesse der Informationssicherheit sollten ermittelt werden. Verantwortlichkeiten für Risikomanagement der Informationssicherheit und insbesondere für die Akzeptanz von Restrisiken sollten definiert werden. Diese Verantwortlichkeiten sollten gegebenenfalls um detaillierte Anleitungen für bestimmte Standorte und Einrichtungen der Informationsverarbeitung erweitert werden. Lokale Verantwortungen für den Schutz organisationseigener Werte und für die Anwendung spezifischer Sicherheitsprozesse sollten definiert werden.

Personen mit Verantwortung für Informationssicherheit dürfen Sicherheitsaufgaben an andere delegieren. Dennoch bleiben sie verantwortlich und sollten feststellen, ob alle übertragenen Aufgaben ordnungsnach durchgeführt wurden.

Die Verantwortungsbereiche von Personen sollten angegeben werden. Insbesondere sollte Folgendes durchgeführt werden:

- a) organisationseigene Werte und Prozesse der Informationssicherheit sollten ermittelt und definiert werden;
- b) die Gesamtverantwortung für jeden organisationseigenen Wert oder Prozess der Informationssicherheit sollte zugeteilt und die Details dieser Verantwortung sollten dokumentiert werden (siehe 8.1.2);
- c) Berechtigungsebenen sollten definiert und dokumentiert werden;
- d) um Verantwortungen im Bereich Informationssicherheit gerecht zu werden, sollten ernannte Personen in diesem Bereich fachkundig sein und die Möglichkeit erhalten, mit Entwicklungen Schritt halten zu können;
- e) Koordination und Kontrolle der Informationssicherheitsaspekte in Lieferantenbeziehungen sollten ermittelt und dokumentiert werden.

Weitere Informationen

Viele Organisationen ernennen einen Manager für Informationssicherheit, der die Gesamtverantwortung für Entwicklung und Umsetzung der Informationssicherheit übernimmt und bei der Identifizierung von Sicherheitsmaßnahmen behilflich ist.

Allerdings verbleibt die Verantwortung für Ermittlung und Implementierung von Sicherheitsmaßnahmen oft bei den einzelnen Managern. Eine gängige Praxis ist es, einen Hauptverantwortlichen für jeden organisationseigenen Wert ernannt, der dann für den laufenden Schutz der Werte verantwortlich ist.

6.1.2 Aufgabentrennung

Maßnahme

Widersprüchliche Aufgaben und Verantwortungsbereiche sollten getrennt werden, um das Risiko unautorisierter oder versehentlicher Änderungen oder Missbrauch organisationseigener Werte zu verringern.

Umsetzungshinweise

Es sollte darauf geachtet werden, dass keine einzelne Person Zugriff auf organisationseigene Werte hat, und sie ohne Genehmigung oder Nachweis modifiziert oder verwendet. Die Einleitung eines Ereignisses sollte von seiner Autorisierung getrennt werden. Die Möglichkeit von Absprachen sollten bei der Gestaltung Sicherheitsmaßnahmen berücksichtigt werden.

Für kleine Organisationen könnte Aufgabentrennung nur mit Schwierigkeiten zu erreichen sein, sollte aber so weit wie möglich oder praktikabel verfolgt werden. Falls Aufgabentrennung nur schwer durchführbar ist, sollten andere Maßnahmen wie Überwachung von Tätigkeiten, Prüfpfade und Leitungsaufsicht in Betracht gezogen werden.

Weitere Informationen

Aufgabentrennung ist eine Methode, um das Risiko versehentlichen oder bewussten Missbrauchs organisationseigener Werte zu verringern.

6.1.3 Kontakt zu Behörden

Maßnahme

Entsprechende Kontakte mit den zuständigen Behörden sollten beibehalten werden.

Umsetzungshinweise

Organisationen sollten über Verfahren verfügen, die festlegen, wann und von wem Behörden (z. B. Strafverfolgungs- und Aufsichtsbehörden) benachrichtigt werden und wie erkannte Informationssicherheitsvorfälle rechtzeitig gemeldet werden (z. B. wenn der Verdacht einer Straftat besteht).

Weitere Informationen

Organisationen, die aus dem Internet angegriffen werden, sind möglicherweise auf Behörden angewiesen, die Schritte gegen die Angriffsquelle einleiten.

Die Pflege solcher Kontakte könnte eine Voraussetzung für die Handhabung von Informationssicherheitsvorfällen (siehe 16) oder für Geschäftskontinuität und Notfallplanung (siehe 17) sein. Kontakte mit Aufsichtsbehörden helfen auch bei der Vorwegnahme und Vorbereitung anstehender Änderungen von Gesetzen und Verordnungen, die von der Organisation umgesetzt werden müssen. Weitere Behörden sind unter anderen, Energieversorgungsbetriebe, Notdienste, Stromversorger, Rettungsdienste z. B. Feuerwehr (Schutz der Geschäftskontinuität), Telekommunikationsanbieter (Kabelschutz und Verfügbarkeit) und Wasserversorger (Kühleinrichtungen für Betriebsmittel).

6.1.4 Kontakt mit Interessengruppen

Maßnahme

Angemessene Kontakte zu Interessenvertretungen oder anderen spezialisierten Sicherheitsforen und Fachverbänden sollten gepflegt werden.

Umsetzungshinweise

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

- a) die Kenntnis über beste Praktiken zu verbessern und über einschlägige Sicherheitsinformationen auf dem Laufenden zu bleiben;
- b) sicherzustellen, dass das Verständnis des Informationssicherheitsumfelds aktuell und vollständig ist;
- c) um rechtzeitig Warnungen, Hinweise und Korrekturen zum Schutz vor Angriffen und Schwachstellen zu erhalten;
- d) um Zugang zu Fachberatung über Informationssicherheit zu erhalten;
- e) um Information über neue Technologien, Produkte, Bedrohungen oder Schwachstellen auszutauschen;
- f) um geeignete Verbindungsstellen beim Umgang mit Informationssicherheitsvorfällen zu bieten (siehe 16).

Weitere Informationen

Vereinbarungen über die gemeinsame Nutzung von Information können eingegangen werden, um die Kooperation bei und die Koordination von Sicherheitsfragen zu verbessern. Solche Vereinbarungen sollten Anforderungen für den Schutz vertraulicher Informationen ermitteln.

6.1.5 Informationssicherheit im Projektmanagement

Maßnahme

Die Informationssicherheit soll ungeachtet der Art des Projekts auch im Projektmanagement berücksichtigt werden.

Umsetzungshinweise

Informationssicherheit sollte in die Projektmanagementmethode(n) einer Organisation integriert werden, damit Risiken in der Informationssicherheit im Rahmen des Projekts identifiziert und behandelt werden können. Dies gilt in der Regel für jede Projektart, z. B. Projekte für Kerngeschäftsprozesse, IT, Gebäudemanagement und andere unterstützende Prozesse. Verwendete Projektmanagementmethoden sollten verlangen dass:

- a) Ziele der Informationssicherheit in den Projektzielen enthalten sind;
- b) eine Risikobewertung der Informationssicherheit in einem frühen Stadium des Projektes durchgeführt wird, um notwendige Sicherheitsmaßnahmen zu identifizieren;
- c) Informationssicherheit Bestandteil aller Phasen der Projektmethodik ist.

Auswirkungen der Informationssicherheit sollten regelmäßig für alle Projekte angesprochen und überprüft werden. Verantwortlichkeiten für Informationssicherheit sollten im Rahmen der Projektmanagementmethoden definiert und spezifischen Funktionen zugewiesen werden.

6.2 Mobilgeräte und Telearbeit

Zielsetzung: Gewährleistung der Sicherheit von Mobilgeräten und Telearbeit.

6.2.1 Leitlinie zu Mobilgeräten

Maßnahme

Eine Leitlinie sollte erstellt und unterstützende Sicherheitsmaßnahmen sollten ergriffen werden, um die Risiken des Einsatzes von Mobilgeräten zu steuern.

Umsetzungshinweise

Bei der Verwendung von Mobilgeräten sollte besonders darauf geachtet werden, dass Unternehmensinformation nicht gefährdet wird. Die Leitlinie für Mobilgeräte sollte die Risiken im Umgang mit Mobilgeräten in einer ungeschützten Umgebung berücksichtigen.

Die Leitlinie für Mobilgeräte sollte berücksichtigen:

- a) Anmeldung von Mobilgeräten;
- b) Anforderungen für den physischen Schutz;
- c) Einschränkung von Software-Installation;
- d) Anforderungen an Software-Versionen der Mobilgeräte und Anwendung von Software-Korrekturen;
- e) Verbindungseinschränkungen zu Informationsdiensten;
- f) Zugangskontrollen;
- g) Verschlüsselungsverfahren;

- h) Schutz vor Schadsoftware;
- i) Remote-Deaktivierung, Löschung oder Sperrung;
- j) Backups;
- k) Nutzung von Internet-Diensten und Internet-Anwendungen.

Bei der Verwendung von Mobilgeräten in öffentlichen Plätzen, Tagungsräumen und anderen ungeschützten Bereichen sollte mit Vorsicht vorgegangen werden. Es sollte ein Schutz vorhanden sein, um unbefugten Zugriff auf Information, die auf diesen Geräten gespeichert und von ihnen verarbeitet werden, und damit ihre Offenlegung zu verhindern, z. B. durch Verwendung von Verschlüsselungsverfahren (siehe 10) und zwingende Anwendung geheimer Authentifizierungsdaten (siehe 9.2.3).

Mobilgeräte sollten auch physisch gegen Diebstahl geschützt sein, insbesondere wenn sie z. B. in Kraftfahrzeugen und anderen Verkehrsmitteln, in Hotels, Konferenzzentren und an Treffpunkten verwendet werden. Für den Fall des Diebstahls oder Verlusts von Mobilgeräten sollte ein spezielles Verfahren unter Berücksichtigung rechtlicher und versicherungstechnischer sowie anderer Sicherheitsanforderungen entwickelt werden. Geräte mit sensiblen oder geschäftskritischen Informationen sollten nicht unbeaufsichtigt gelassen und wenn möglich unter Verschluss gehalten oder mit Spezialschlössern gesichert werden.

Für das Personal sollten Schulungen arrangiert werden, um das Bewusstsein für zusätzliche Risiken bei der Arbeit mit diesen Geräten und einzusetzenden Sicherheitsmaßnahmen zu schärfen.

Falls die Leitlinie für Mobilgeräte die Nutzung von privaten Mobilgeräten erlaubt, müssen Leitlinie und zugehörige Sicherheitsmaßnahmen auch folgendes berücksichtigen:

- a) Trennung von privater und geschäftlicher Nutzung der Geräte, einschließlich Software in Unterstützung dieser Trennung und zum Schutz von geschäftlichen Daten auf privaten Geräten;
- b) Zugriff auf geschäftliche Daten erst, nachdem Benutzer einen Endnutzervertrag unterzeichnet haben, in dem sie ihre Pflichten anerkennen (physischer Schutz, Software-Aktualisierung), ihren Verzicht auf das Eigentum von Geschäftsdaten erklären, damit die Organisation im Fall des Diebstahls oder Verlusts des Gerätes oder des Entzugs der Nutzungsberechtigung diese Daten per Fernzugriff löschen darf. Diese Leitlinie muss das Datenschutzrecht berücksichtigen.

Weitere Informationen

Drahtlose Verbindungen mit Mobilgeräten sind anderen Arten von Netzwerkverbindungen ähnlich, zeigen allerdings wesentliche Unterschiede, die bei der Ermittlung von Sicherheitsmaßnahmen berücksichtigt werden sollten. Typische Unterschiede sind:

- a) einige Sicherheitsprotokolle für drahtlose Verbindungen sind nicht ausgereift und haben bekannte Schwächen;
- b) auf Mobilgeräten gespeicherte Information kann aufgrund begrenzter Netzwerkbandbreite nicht gesichert werden oder Mobilgeräte sind zum Zeitpunkt der geplanten Sicherung nicht angeschlossen.

Mobilgeräte verfügen in der Regel über die gleichen Funktionen wie ortsfeste Geräte, z. B. Vernetzung, Internet, E-Mail und Dateioperationen. Sicherheitsmaßnahmen für Informationssicherheit von Mobilgeräten bestehen in der Regel aus Maßnahmen für ortsfeste Geräte und solchen, die Bedrohungen durch die Verwendung außerhalb des Geländes der Organisation abwenden.

6.2.2 Telearbeit

Maßnahme

Es sollten eine Leitlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen festgelegt werden, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden.

Umsetzungshinweise

Organisationen, die Telearbeit erlauben, sollten eine Leitlinie zur Definition von Bedingungen und Einschränkungen der Telearbeit erlassen. Soweit erforderlich und gesetzlich zulässig, sollten folgende Fragen berücksichtigt werden:

- a) die bestehende physische Sicherheit des Telearbeitsstandortes unter Berücksichtigung der physischen Sicherheit des Gebäudes und der lokalen Umgebung;
- b) die vorgeschlagene physikalische Telearbeitsumgebung;
- c) die Sicherheitsanforderungen für die Kommunikation, unter Berücksichtigung des notwendigen Fernzugriffs auf interne organisationseigene Systeme, die Sensibilität der abgerufenen Information und deren Weitergabe über Telekommunikationsverbindungen sowie die Empfindlichkeit der internen Systeme;
- d) die Bereitstellung von virtuellem Desktop-Zugriff, der Verarbeitung und Speicherung von Information auf privaten Geräten unterbindet;
- e) die Gefahr des unbefugten Zugriffs auf Informationen durch andere, mit dem Benutzer lebende Personen, z. B. Familie und Freunde;
- f) die Verwendung von Heimnetzwerken und Anforderungen und Beschränkungen der Konfiguration von drahtlosen Netzwerkdiensten;
- g) Richtlinien und Verfahren, um Streitigkeiten über Rechte an geistigem Eigentum zu verhindern, das auf privaten Geräten erarbeitet wurde;
- h) Zugang zu privaten Geräten (um die Sicherheit des Rechners oder während einer Untersuchung zu überprüfen), der vom Gesetzgeber verhindert werden könnte;
- i) Software-Lizenzvereinbarungen, die so festgelegt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Rechnern von Mitarbeitern oder externen Benutzern verantwortlich sein könnten;
- j) Anforderungen an Virenschutz und Firewall.

Die zu berücksichtigen Richtlinien und Regelungen sollten enthalten:

- a) die Bereitstellung geeigneter Betriebsmittel und Lagerungseinrichtungen für Telearbeit, wobei der Einsatz von privaten, nicht unter der Kontrolle der Organisation stehenden Geräten untersagt ist;
- b) die Festlegung gestatteter Arbeit, die Arbeitszeit, die Klassifizierung aufbewahrter Informationen und interne Systeme und Dienste, auf die der Telearbeiter berechtigterweise Zugriff hat;
- c) die Bereitstellung geeigneter Telekommunikationseinrichtungen, einschließlich Methoden zur Sicherung des Fernzugriffs;
- d) physische Sicherheit;
- e) Regeln und Leitlinien für den Zugang von Familie und Besuchern zu Betriebsmitteln und Informationen;

- f) die Bereitstellung von Betreuung und Wartung für Hard-und Software;
- g) Bereitstellung von Versicherung;
- h) Verfahren für Backups und Geschäftskontinuität;
- i) Prüfung und Überwachung der Sicherheit;
- j) Widerruf von Berechtigungen und Zugriffsrechten sowie die Rückgabe von Betriebsmitteln nach Beendigung der Telearbeitsvereinbarung.

Weitere Informationen

Telearbeit bezieht sich auf alle Formen der Arbeit außerhalb des Büros, einschließlich neuartiger Arbeitsumgebungen wie „Heimarbeit“, „flexibler Arbeitsplatz“, „Remote-Arbeit“ und „virtuelle Arbeit“.

7 Personalsicherheit

7.1 Vor der Anstellung

Zielsetzung: Sicherstellung, dass Mitarbeiter und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Positionen geeignet sind.

7.1.1 Überprüfung

Maßnahme

Der Hintergrund von allen Bewerbern sollte im Einvernehmen mit einschlägigen Gesetzen, Verordnungen und ethischen Grundsätzen geprüft werden. Prüfungen sollten in einem angemessenen Verhältnis zu Geschäftsanforderungen, der Klassifikation der aufzurufenden Informationen und zum vermeintlichen Risiko stehen.

Umsetzungshinweise

Überprüfungen sollten alle Rechtsvorschriften über Datenschutz, Schutz der Privatsphäre und Arbeitsschutz berücksichtigen und, sofern erlaubt, Folgendes einschließen:

- a) Vorhandensein zufriedenstellender Leumundszeugnisse, z. B. ein geschäftsbezogenes und ein privates Zeugnis;
- b) ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers und;
- c) Bestätigung angegebener akademischer und beruflicher Qualifikationen;
- d) unabhängige Identitätsüberprüfung (Reisepass oder ähnliches Dokument);
- e) detailliertere Nachweise, wie Bonitätsprüfung oder Überprüfung des Strafregisters.

Wenn eine Person für eine bestimmte Funktion der Informationssicherheit angestellt wird, sollten Organisationen sicherstellen, dass der Bewerber:

- a) über die notwendige Kompetenz für die Sicherheitsaufgabe verfügt;
- b) über die erforderliche Vertrauenswürdigkeit verfügt, insbesondere wenn die Funktion von entscheidender Bedeutung für die Organisation ist.

Falls eine ersteingestellte oder beförderte Person Zugang zu informationsverarbeitenden Einrichtungen hat, die insbesondere vertrauliche Informationen verarbeiten, wie finanzielle oder streng vertrauliche Daten, sollte die Organisation weitere, eingehendere Prüfungen in Betracht ziehen.

Verfahren sollten Kriterien und Einschränkungen zur Überprüfung von Nachweisen definieren, z. B. wer ist berechtigt, Bewerber zu überprüfen und wie, wann und warum Nachweise überprüft werden.

Auftragnehmer sollten auch überprüft werden. In diesen Fällen sollte die Verantwortung für Überprüfungen zwischen Organisation und Auftragnehmer vereinbart und Meldeverfahren festgelegt werden, die bei noch nicht abgeschlossener Überprüfung oder bei zu Zweifel oder Bedenken Anlass gebenden Ergebnissen befolgt werden müssen.

Informationen über alle für Positionen in der Organisation infrage kommenden Bewerber sollten im Einvernehmen mit entsprechenden Gesetzen in der jeweiligen Rechtsordnung gesammelt und verarbeitet werden. Je nach geltender Rechtsvorschrift sollten die Bewerber im voraus über Prüfungsverfahren informiert werden.

7.1.2 Arbeitsvertragsklauseln

Maßnahme

Die Vereinbarungen zwischen Organisation und Mitarbeitern sollten die Verantwortlichkeiten für Informationssicherheit beider Parteien angeben.

Umsetzungshinweise

Die vertraglichen Verpflichtungen der Mitarbeiter oder Auftragnehmer sollte die Leitlinie für Informationssicherheit der Organisation widerspiegeln und außerdem Folgendes klären und angeben:

- a) dass alle Mitarbeiter und Auftragnehmer, Zugang zu vertraulichen Informationen erhalten, eine Vertraulichkeitserklärung oder Geheimhaltungsvereinbarung unterzeichnen, bevor sie Zugang zu Einrichtungen zur Informationsverarbeitung erhalten (siehe 13.2.4);
- b) gesetzliche Pflichten und Rechte der Mitarbeiter oder Auftragnehmer, z. B. bezüglich Urheberrechtsgesetzen oder Datenschutzgesetzgebung (siehe 18.1.4);
- c) Verantwortungen für die Klassifizierung von Informationen und die Verwaltung organisationseigener Werte, die mit Informationen, Einrichtungen zur Informationsverarbeitung und Informationsdiensten assoziiert sind, die von Mitarbeitern und Auftragnehmern verarbeitet werden (siehe 8);
- d) Zuständigkeiten der Mitarbeiter oder Auftragnehmer für den Umgang mit Informationen, die von anderen Unternehmen oder externen Parteien zur Verfügung gestellt wurden;
- e) Maßnahmen, die ergriffen werden müssen, falls die Mitarbeiter oder Auftragnehmer die Sicherheitsanforderungen der Organisation ignorieren (siehe 7.2.3).

Rollen und Verantwortlichkeiten der Informationssicherheit sollten Bewerbern im Laufe des Einstellungsverfahrens mitgeteilt werden.

Die Organisation sollte sicherstellen, dass Mitarbeiter und Auftragnehmer den Bedingungen und Konditionen für Informationssicherheit zustimmen. Bedingungen und Konditionen sollten Art und Umfang des Zugangs zu organisationseigenen Werten im Zusammenhang mit Informationssystemen und -diensten berücksichtigen.

Gegebenenfalls sollten Verantwortlichkeiten, die in den Beschäftigungsbedingungen angegeben sind, über die Beschäftigungsdauer hinaus für einen bestimmten Zeitraum gelten (siehe 7.3).

Weitere Informationen

Ein Verhaltenskodex kann verwendet werden, um die Zuständigkeiten für Informationssicherheit der Mitarbeiter und Auftragnehmer in Bezug auf Geheimhaltung, Datenschutz, ethische Grundsätze, angemessene Nutzung von Betriebsmitteln und Einrichtungen sowie von der Organisation erwartete, seriöse Praktiken anzugeben. Von der externen Partei, mit der ein Auftragnehmer assoziiert ist, kann verlangt werden, eine Vereinbarung im Namen der verpflichteten Person einzugehen.

7.2 Während der Anstellung

Zielsetzung: Sicherstellung, dass Mitarbeiter und Auftragnehmer sich ihrer Verantwortung für Informationssicherheit bewusst sind und ihr nachkommen.

7.2.1 Verantwortung des ManagementsMaßnahme

Das Management sollte alle Mitarbeiter und Auftragnehmer dazu anhalten, Sicherheitsmaßnahmen entsprechend den festgelegten Leitlinien und Verfahren der Organisation anzuwenden.

Umsetzungshinweise

Führungsverantwortung sollte unter anderen beinhalten, dass Mitarbeiter und Auftragnehmer:

- a) vor Zugangsgewährung zu vertraulicher Information und Informationssystemen genau über ihre Funktionen und Zuständigkeiten in der Informationssicherheit informiert werden;
- b) Leitlinien erhalten, die die Erwartungen an ihre Rolle in der Informationssicherheit innerhalb der Organisation darlegen;
- c) motiviert sind, den Leitlinien für Informationssicherheit der Organisation gerecht zu werden;
- d) eine Bewusstseinsebene für Informationssicherheit erreichen, die ihren Funktionen und Zuständigkeiten in der Organisation entspricht (siehe 7.2.2);
- e) den Beschäftigungsbedingungen entsprechen, einschließlich der Leitlinie zur Informationssicherheit der Organisation und geeigneten Arbeitsmethoden;
- f) auch in Zukunft angemessene Fähigkeiten und Qualifikationen besitzen und regelmäßig weitergebildet werden;
- g) anonym über Verletzungen von Leitlinien und Verfahren zur Informationssicherheit Bericht erstatten können („whistle blowing“).

Management sollte Leitlinien, Verfahren und Kontrollen zur Informationssicherheit unterstützen und Vorbild sein.

Weitere Informationen

Falls sich Mitarbeiter und Auftragnehmer nicht der Zuständigkeiten für Informationssicherheit bewusst sind, kann dies zu erheblichem Schaden für die Organisation führen. Motivierte Mitarbeiter sind voraussichtlich zuverlässiger und verursachen weniger Informationssicherheitsvorfälle.

Schlechtes Management kann dazu führen, dass sich das Personal unterbewertet fühlt, mit negativen Folgen für die Informationssicherheit der Organisation. Zum Beispiel kann schlechtes Management zu einer Vernachlässigung der Informationssicherheit oder zu einem potenziellen Missbrauch der organisationseigenen Werte führen.

7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit

Maßnahme

Alle Mitarbeiter der Organisation sowie gegebenenfalls Auftragnehmer sollten in geeigneter Weise aufgeklärt und geschult werden und regelmäßige Ergänzungen zu organisatorischen Leitlinien und Verfahren erhalten, die für ihre berufliche Funktion maßgebend sind.

Umsetzungshinweise

Ein Sensibilisierungsprogramm für Informationssicherheit sollte darauf abzielen, dass sich Mitarbeiter und gegebenenfalls Auftragnehmer ihrer Verantwortung für Informationssicherheit bewusst werden und auf welche Weise diesen Verantwortungen entsprochen wird.

Ein Sensibilisierungsprogramm für Informationssicherheit sollte in Einklang mit Leitlinien und relevanten Verfahren der Organisation, unter Berücksichtigung der zu schützenden Information der Organisation und der schon bestehenden Sicherheitsmaßnahmen zum Schutz der Information festgelegt werden. Das Sensibilisierungsprogramm sollte eine Reihe von Sensibilisierungsmaßnahmen enthalten, wie Kampagnen (z. B. Tag der Informationssicherheit) und das Herausgeben von Broschüren und Rundschreiben.

Das Sensibilisierungsprogramm sollte unter Berücksichtigung von Mitarbeiterfunktionen in der Organisation und gegebenenfalls unter Berücksichtigung der organisationseigenen Erwartungen an die Sensibilisierung von Auftragnehmern geplant werden. Maßnahmen des Sensibilisierungsprogramms sollten vorher genau und regelmäßig eingeplant werden, damit Maßnahmen wiederholt und dadurch auch neuen Mitarbeitern und Auftragnehmern angeboten werden können. Das Sensibilisierungsprogramm sollte regelmäßig aktualisiert werden, um in Einklang mit Leitlinien und Verfahren der Organisation zu bleiben und sollte außerdem auf gewonnenen Erkenntnissen aus Informationssicherheitsvorfällen basieren.

Sensibilisierungsschulung sollte nach dem Sensibilisierungsprogramm für Informationssicherheit der Organisation durchgeführt werden. Sensibilisierungsschulung kann auf unterschiedliche Wege durchgeführt werden, darunter Klassenunterricht, Fernunterricht, internetbasiert, Selbststudium und andere.

Aus- und Weiterbildung in Informationssicherheit sollte generelle Aspekte enthalten wie:

- a) Darlegung der Verpflichtung des Managements zu Informationssicherheit in der gesamten Organisation;
- b) die Notwendigkeit, mit geltenden Regeln und Verpflichtungen der Informationssicherheit vertraut zu werden und sie zu beachten, wie in Richtlinien, Normen, Gesetzen, Verordnungen, Verträgen und Vereinbarungen festgelegt;
- c) persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Aufgaben zur Sicherung oder zum Schutz von Informationen, die der Organisation und externen Parteien gehören;
- d) grundsätzliche Verfahren zur Informationssicherheit (Berichterstattung über Informationssicherheitsvorfälle) und grundlegende Sicherheitsmaßnahmen (Kennwortsicherheit, Maßnahmen bei Schadsoftware und aufgeräumter Schreibtisch);
- e) Anlaufstellen und Ressourcen für zusätzliche Informationen und Empfehlungen zu Fragen der Informationssicherheit, einschließlich weiterer Aus- und Weiterbildungsunterlagen zur Informationssicherheit.

Aus- und Weiterbildung zur Informationssicherheit sollte regelmäßig stattfinden. Eine anfängliche Aus- und Weiterbildung gilt nicht nur für Neuanfänger, sondern auch für Mitarbeiter, die in anderen Positionen oder Funktionen mit deutlich unterschiedlichen Anforderungen an Informationssicherheit versetzt wurden, und sollte vor der Versetzung stattfinden.

Für eine wirkungsvolle Aus- und Weiterbildung sollte ein Programm entwickelt werden. Das Programm sollte in Einklang sein mit Leitlinien und relevanten Verfahren der Organisation, unter Berücksichtigung der zu schützenden Information der Organisation und der schon bestehenden Sicherheitsmaßnahmen zum Schutz

der Information. Das Programm sollte unterschiedliche Formen der Aus- und Weiterbildung in Betracht ziehen, z. B. Vorträge oder Selbststudium.

Weitere Informationen

Bei der Ausarbeitung eines Aus- und Weiterbildungsprogramms ist wichtig, nicht nur das „Was“ und „Wie“, sondern auch das „Warum“ anzusprechen. Es ist wichtig, dass Mitarbeiter das Ziel der Informationssicherheit und der möglichen positiven und negativen Auswirkungen auf die Organisation verstehen.

Sensibilisierung, Aus- und Weiterbildung können im Rahmen anderer Ausbildungsmaßnahmen durchgeführt werden, z. B. des allgemeinen IT- oder Sicherheitstrainings. Sensibilisierung, Aus- und Weiterbildung sollten für die Aufgaben, Verantwortlichkeiten und Fähigkeiten der Person angemessen und relevant sein (siehe 7.2.2).

Eine Beurteilung des Verständnisses der Mitarbeiter könnte mit einem Wissenstest am Ende des Sensibilisierungs-, Aus- und Weiterbildungskurses durchgeführt werden.

7.2.3 Disziplinarverfahren

Maßnahme

Ein offizielles, festgelegtes Verfahren sollte vorhanden sein, um disziplinarische Maßnahmen gegen Mitarbeiter einzuleiten, die gegen die Informationssicherheit verstoßen haben.

Umsetzungshinweise

Ein Disziplinarverfahren sollte nicht ohne vorherige Prüfung eingeleitet werden, dass eine Informationssicherheitsverletzung aufgetreten ist (siehe 16.1.7).

Ein formelles Disziplinarverfahren sollte eine korrekte und faire Behandlung der Mitarbeiter sicherstellen, die verdächtigt werden, eine Verletzung der Informationssicherheit begangen zu haben. Ein formelles Disziplinarverfahren sollte eine abgestufte Reaktion erlauben, unter Berücksichtigung der Art und Schwere der Verletzung und ihrer Auswirkung auf das Unternehmen, unabhängig davon, ob es der erste Verstoß oder eine Rückfälligkeit ist, oder ob die beschuldigte Person entsprechend geschult war. Außerdem sollten die einschlägige Gesetzgebung, Geschäftsverträge und gegebenenfalls andere Faktoren in Betracht gezogen werden.

Ein Disziplinarverfahren sollte ebenfalls eine abschreckende Wirkung haben, um Mitarbeiter davon abzuhalten, Leitlinien und Verfahren zur Informationssicherheit der Organisation zu verletzen, oder gegen andere Maßnahmen zur Informationssicherheit zu verstoßen. Vorsätzliche Verstöße erfordern möglicherweise unverzügliche Maßnahmen.

Weitere Informationen

Ein Disziplinarverfahren kann auch eine Motivation oder Ansporn werden, wenn positive Maßnahmen für bemerkenswertes Verhalten in Bezug auf Informationssicherheit definiert sind.

7.3 Beendigung und Wechsel der Anstellung

Zielsetzung: Schutz der Interessen der Organisation bei einem Wechsel oder der Beendigung der Anstellung.

7.3.1 Zuständigkeiten bei Beendigung oder Wechsel der Anstellung

Maßnahme

Zuständigkeiten und Pflichten zur Informationssicherheit, die nach Beendigung oder Veränderung des Arbeitsverhältnisses in Kraft bleiben sollen, sollten festgelegt, dem Mitarbeiter oder Auftragnehmer mitgeteilt und umgesetzt werden.

Umsetzungshinweise

Die Mitteilung von Verantwortlichkeiten im Zusammenhang mit der Beendigung des Arbeitsverhältnisses sollte bereits geltende Sicherheitsanforderungen und rechtliche Verpflichtungen als auch ggf. Verpflichtungen aufgrund einer Vertraulichkeitsverpflichtung (siehe 13.2.4) und der Beschäftigungsbedingungen (siehe 7.1.2) beinhalten, die für einen festgelegten Zeitraum nach Ende des Anstellungs- bzw. Auftragnehmerverhältnisses fortgelten.

Die nach Beendigung des Arbeitsverhältnisses weitergeltenden Verantwortlichkeiten und Pflichten sollten in den Beschäftigungsbedingungen des Mitarbeiters bzw. Auftragnehmers beschrieben werden (siehe 7.1.2).

Änderungen des Verantwortungsbereichs oder des Beschäftigungsverhältnisses sollten geregelt und die Entbindung vom aktuellen Verantwortungsbereich bzw. Beschäftigungsverhältnis sollte kombiniert werden mit der Betrauung mit einem neuen Verantwortungsbereich bzw. dem Beginn eines neuen Beschäftigungsverhältnisses.

Weitere Informationen

Die Personalabteilung ist im Allgemeinen zuständig für den gesamten Beendigungsprozess und arbeitet mit dem Vorgesetzten der ausscheidenden Person zusammen, um Aspekte der Informationssicherheit im Zusammenhang mit den entsprechenden Verfahren zu regeln. Falls ein Auftragnehmer von einer externen Partei beauftragt wurde, wird dieser Beendigungsprozess von der externen Partei entsprechend dem Vertrag zwischen der Organisation und der externen Partei betrieben.

Unter Umständen ist es erforderlich, Mitarbeiter, Kunden oder Auftragnehmer über Veränderungen im Personal- und betrieblichen Bereich zu informieren.

8 Management von organisationseigenen Werten

8.1 Verantwortung für organisationseigene Werte

Zielsetzung: Feststellung unternehmenseigener Werte und Festlegung entsprechender Verantwortlichkeiten zu deren Schutz.

8.1.1 Inventar der organisationseigenen Werte

Maßnahme

Werte, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, müssen ermittelt werden, und von diesen Anlagen ist ein Inventar zu erstellen und zu pflegen.

Umsetzungshinweise

Eine Organisation sollte Werte ermitteln, die relevant für den Informationslebenszyklus sind und ihre Wichtigkeit dokumentieren. Der Lebenszyklus von Informationen sollte Erstellung, Verarbeitung, Speicherung, Übermittlung, Löschung und Zerstörung umfassen. Die Dokumentation sollte in eigenen oder ggf. bestehenden Inventaren aufbewahrt werden.

Das Inventar der Werte sollte genau, aktuell und konsistent sowie mit anderen Inventaren abgestimmt sein.

Bei jedem der festgestellten Werte müssen der Eigentümer benannt (siehe 8.1.2), und die Klassifizierung festgestellt werden (siehe 8.2).

Weitere Informationen

Die Inventaraufzeichnungen der Werte tragen dazu bei sicherzustellen, dass ein wirksamer Schutz existiert und können außerdem für weitere Zwecke wie Gesundheits- und Arbeitsschutz sowie Versicherungs- oder Finanzfragen (Wertemanagement) erforderlich sein.

ISO/IEC 27005 bietet Beispiele von Werten, die von der Organisation bei der Ermittlung von Werten möglicherweise in Betracht gezogen werden müssen. Der Vorgang der Zusammenstellung eines Inventars unternehmenseigener Wert ist eine wichtige Voraussetzung für das Risikomanagement (siehe auch ISO/IEC 27000 und ISO/IEC 27005).

8.1.2 Eigentum von organisationseigenen Werten

Maßnahme

Für im Inventar geführte Werte muss es Eigentümer geben.

Umsetzungshinweise

Natürliche als auch juristische Personen mit bestätigter Management-Verantwortung für den Lebenszyklus des Wertes können zu Eigentümern der Werte bestimmt werden.

Ein Verfahren zur Sicherstellung einer zeitnahen Bestimmung der Eigentümerschaft ist normalerweise implementiert. Die Eigentümerschaft sollte zugewiesen werden, wenn Werte geschaffen oder auf die Organisation übertragen werden. Der Werteeigentümer sollte für die ordnungsgemäße Verwaltung des Wertes über dessen gesamten Lebenszyklus verantwortlich sein.

Der Werteeigentümer sollte:

- a) sicherstellen, dass die Werte inventarisiert werden;
- b) sicherstellen, dass die Werte angemessen klassifiziert und geschützt werden;
- c) Zugangsbeschränkungen und Klassifizierungen wichtiger Werte festlegen und regelmäßig überprüfen, unter Berücksichtigung der geltenden Zugangskontrollleitlinien;
- d) einen ordnungsgemäßen Umgang bei der Löschung oder Zerstörung des Wertes sicherstellen.

Weitere Informationen

Bei dem festgestellten Eigentümer kann es sich entweder um eine natürliche oder juristische Person mit bestätigter Management-Verantwortung für den kompletten Lebenszyklus eines Wertes handeln. Der festgestellte Eigentümer verfügt nicht unbedingt im juristischen Sinne über Eigentumsrechte am Wert.

Routineaufgaben können delegiert werden. So kann beispielsweise ein Verwalter die Werte beaufsichtigen, die rechtliche Verantwortung verbleibt jedoch beim Eigentümer.

Bei komplexen Informationssystemen kann es sinnvoll sein, Gruppen von Werten zu bestimmen, die zusammen eine bestimmte Dienstleistung darstellen. In diesem Fall ist der Eigentümer dieser Dienstleistung für die Erbringung der Dienstleistung verantwortlich, einschließlich des Betriebs der Werte.

8.1.3 Zulässiger Gebrauch von organisationseigenen Werten

Maßnahme

Es sollten Regeln für den zulässigen Gebrauch von Informationen und Werten, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, aufgestellt, dokumentiert und implementiert werden.

Umsetzungshinweise

Mitarbeiter und Benutzer von externen Parteien, die die Werte der Organisation nutzen oder Zugang zu ihnen haben, sollten auf die Informationssicherheitsanforderungen hinsichtlich der mit Informationen und Einrichtungen und Ressourcen zur Informationsverarbeitung verbundenen Werte der Organisation hingewiesen werden. Sie sollten für ihre eigene Nutzung informationsverarbeitender Ressourcen verantwortlich sein, und jedwede derartige Nutzung hat unter ihrer Verantwortung zu erfolgen.

8.1.4 Rückgabe von organisationseigenen Werten

Maßnahme

Alle Mitarbeiter und externen Benutzer sollten sämtliche Werte der Organisation zurückgeben, die sich bei Auslauf ihrer Anstellung oder ihres Vertrags noch in ihrem Besitz befinden.

Umsetzungshinweise

Der Beendigungsprozess sollte dergestalt formalisiert sein, dass er die Rückgabe aller zuvor ausgegebenen physischen und elektronischen Werte einschließt, die Eigentum der Organisation sind oder dieser anvertraut wurden.

In Fällen, in denen ein Mitarbeiter oder eine externe Partei Betriebsmittel der Organisation erwirbt oder seine eigene Ausrüstung benutzt, sollten Verfahren eingehalten werden, durch die sichergestellt ist, dass alle relevanten Informationen an die Organisation übermittelt und sicher von den Betriebsmitteln gelöscht werden (siehe 11.2.7).

In Fällen, in denen ein Mitarbeiter oder eine externe Partei über Kenntnisse verfügt, die wichtig für den laufenden Betrieb sind, sollten diese Informationen dokumentiert und an die Organisation übermittelt werden.

Während der Kündigungsfrist sollte die Organisation Kontrollen einrichten, um nicht genehmigtes Kopieren relevanter Informationen (z. B. geistiges Eigentum) durch scheidende Mitarbeiter und Auftragnehmer zu verhindern.

8.2 Klassifizierung von Informationen

Zielsetzung: Sicherstellung, dass Informationen eine angemessene Schutzstufe entsprechend ihrer Bedeutung für die Organisation zugeteilt bekommen.

8.2.1 Klassifizierung von Informationen

Maßnahme

Informationen sollten nach ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit und Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung klassifiziert werden.

Umsetzungshinweise

Bei den Klassifizierungen und den damit verbundenen Sicherheitsmaßnahmen zugunsten der Informationen sollten die geschäftlichen Anforderungen bezüglich der gemeinsamen Nutzung von bzw. der Einschränkung des Zugriffs auf Informationen sowie die gesetzlichen Vorschriften berücksichtigt werden. Werte, bei denen es sich nicht um Informationen handelt, können auch entsprechend der Klassifizierung der darin gespeicherten, von diesen verarbeiteten oder auf andere Weise gehandhabten oder geschützten Informationen klassifiziert werden.

Die Eigentümer von Informationswerten sollten für ihre Klassifizierung verantwortlich sein.

Das Klassifizierungsschema sollte Konventionen für die Klassifizierung und Kriterien zur Überprüfung der Klassifizierung in bestimmten zeitlichen Abständen beinhalten. Die Schutzstufe innerhalb des Schemas mittels Analyse der Vertraulichkeit, Integrität und Verfügbarkeit sowie jedweder sonstiger Anforderungen bezüglich der jeweiligen Informationen bestimmt werden. Das Schema sollte auf die Zugangskontrollleitlinie (siehe 9.1.1) abgestimmt sein.

Jeder Stufe sollte eine Bezeichnung zugewiesen werden, die im Zusammenhang mit der Anwendung des Klassifizierungsschemas Sinn ergibt.

Das Schema sollte einheitlich innerhalb der gesamten Organisation sein, damit Informationen und zugehörige Werte überall einheitlich klassifiziert werden, ein gemeinsames Verständnis von Schutzanforderungen besteht und ein angemessener Schutz Anwendung findet.

Die Klassifizierung sollte in die Prozesse der Organisation einbezogen werden und innerhalb der gesamten Organisation konsistent und kohärent sein. Ergebnis der Klassifizierung sollte die Einstufung von Werten in Abhängigkeit von ihrer Sensibilität und Betriebswichtigkeit für die Organisation, z. B. hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit, sein. Die Ergebnisse der Klassifizierung sollten bei Änderungen des materiellen Werts, der Sensibilität und der Betriebswichtigkeit im Laufe des Lebenszyklus aktualisiert werden.

Weitere Informationen

Die Klassifizierung bietet Personen im Umgang mit Informationen eine prägnante Angabe zu deren Handhabung und Schutz. Durch die Definition von Informationsgruppen mit ähnlichen Schutzanforderungen sowie Spezifizierung der für alle Informationen der jeweiligen Gruppen geltenden Informationssicherheitsverfahren wird dies zusätzlich vereinfacht. Durch diesen Ansatz reduziert sich der Aufwand für fallbezogene Risikoeinschätzungen und die Planung von Einzelmaßnahmen zur Gewährleistung der Sicherheit.

Informationen können ihren sensiblen oder betriebswichtigen Charakter nach einer gewissen Zeitspanne verlieren, z. B. wenn sie öffentlich gemacht wurden. Diese Aspekte sollten in Betracht gezogen werden, da eine Überklassifizierung zur Umsetzung unnötiger Sicherheitsmaßnahmen führen kann, die zusätzliche Ausgaben zur Folge haben. Auf der anderen Seite kann eine Unterklassifizierung die Erreichung der Geschäftsziele gefährden.

Als Beispiel für ein Klassifizierungsschema zur Vertraulichkeit von Informationen kann das folgende, vierstufige Modell dienen:

- a) Offenlegung ist gefahrlos möglich;
- b) Offenlegung führt zu geringfügigen Verlegenheiten oder geringfügigen betrieblichen Unannehmlichkeiten;
- c) Offenlegung hat signifikante, kurzfristige Auswirkungen auf den Betriebsablauf oder taktische Ziele;
- d) Offenlegung hat schwerwiegende Auswirkungen auf langfristige strategische Zielsetzungen und gefährdet den Bestand der Organisation.

8.2.2 Kennzeichnung von Informationen

Maßnahme

Eine angemessene Anzahl von Verfahren zur Kennzeichnung von Informationen ist entsprechend dem von der Organisation übernommenen Klassifizierungsschema für Informationen zu entwickeln und zu implementieren.

Umsetzungshinweise

Verfahren zur Kennzeichnung von Informationen müssen sich auf die Informationen selbst sowie auf zugehörige Werte in physischem und elektronischem Format beziehen. Die Kennzeichnung sollte dem in 8.2.1 festgelegten Klassifizierungsschema Rechnung tragen. Die Kennzeichnungen sollten gut zu erkennen sein. Die Verfahren sollten eine Anleitung bieten, wo und wie Kennzeichnungen anzubringen sind unter Berücksichtigung der Art und Weise, wie auf die Informationen zugegriffen wird bzw. der Umgang mit den Werten in Abhängigkeit vom jeweiligen Medientyp erfolgt. In den Verfahren können Fälle festgelegt sein, in denen auf eine Kennzeichnung verzichtet wird, z. B. bei nicht vertraulichen Informationen, um die Arbeitsbelastung zu verringern. Mitarbeiter und Auftragnehmer sollten auf die Kennzeichnungsverfahren aufmerksam gemacht werden.

Ausgabedaten von Systemen, die als sensibel oder betriebswichtig eingestufte Informationen enthalten, sollten auf ihrer Ausgabeseite eine entsprechende Klassifizierungskennzeichnung tragen.

Weitere Informationen

Die Kennzeichnung klassifizierter Informationen stellt eine wesentliche Voraussetzung für Vereinbarungen zu deren gemeinsamer Nutzung dar. Physische Kennzeichnungen und Metadaten sind eine übliche Kennzeichnungsform.

Die Kennzeichnung von Informationen und zugehöriger Werte kann unter Umständen negative Auswirkungen haben. Klassifizierte Werte sind einfacher zu erkennen und dementsprechend einfacher von internen Personen oder Angreifern von außen zu entwenden.

8.2.3 Handhabung von organisationseigenen Werten

Maßnahme

Verfahren für den Umgang mit Werten sind entsprechend dem von der Organisation übernommenen Klassifizierungsschema für Informationen zu entwickeln und zu implementieren.

Umsetzungshinweise

Die Verfahren sollten die Handhabung, Verarbeitung, Speicherung und Kommunizierung von Informationen entsprechend ihrer Klassifizierung vorsehen (siehe 8.2.1).

Die folgenden Punkte sollten dabei berücksichtigt werden:

- a) Zugriffsbeschränkungen zur Unterstützung der Schutzanforderungen für jede Klassifizierungsstufe;
- b) Pflege eines offiziellen Verzeichnisses der autorisierten Empfänger von Werten;
- c) Schutz temporärer oder dauerhafter Kopien von Informationen in einer Weise, die dem Schutz der Originalinformationen entspricht;
- d) Speicherung von IT-Assets nach den Herstellerspezifikationen;
- e) deutliche Kennzeichnung sämtlicher Datenträgerkopien als Hinweis für den autorisierten Empfänger.

Das innerhalb der Organisation verwendete Klassifizierungsschema ist möglicherweise nicht äquivalent zu jenen anderer Organisationen, selbst wenn die Bezeichnungen einzelner Stufen ähnlich sind. Außerdem kann sich die Klassifizierung von zwischen den Organisationen ausgetauschten Informationen je nach Kontext in der jeweiligen Organisation unterscheiden, auch wenn die beiden Klassifizierungsschemata identisch sind.

Vereinbarungen mit anderen Organisationen, die den Austausch von Informationen einschließen, sollten daher Verfahren zur Feststellung der Klassifizierung der betreffenden Informationen und zur Interpretation der Klassifizierungskennzeichnungen anderer Organisationen vorsehen.

8.3 Handhabung von Speicher- und Aufzeichnungsmedien

Zielsetzung: Verhinderung unerlaubter Offenlegung, Veränderung, Entfernung oder Zerstörung von Informationen, die auf Medien gespeichert sind.

8.3.1 Verwaltung von Wechselmedien

Maßnahme

Es sollten Verfahren für die Verwaltung von Wechselmedien entsprechend dem von der Organisation übernommenen Klassifizierungsschema implementiert werden.

Umsetzungshinweise

Die folgenden Leitlinien für die Verwaltung von Wechselmedien sollten beachtet werden:

- a) Nicht mehr benötigte Inhalte auf wiederverwertbaren Medien, die aus der Organisation entfernt werden müssen, sollten so gelöscht werden, dass sie nicht wiederherstellbar sind;
- b) Sofern dies notwendig und praktikabel ist, sollten eine Genehmigung für die Entfernung von Medien aus der Organisation und Aufzeichnungen über die Entfernung zur Auflage gemacht werden, um einem Prüfpfad zu entsprechen;
- c) Sämtliche Medien sollten in einer sicheren und abgesicherten Umgebung aufbewahrt werden, die den Herstellerspezifikationen entspricht;
- d) Wenn die Vertraulichkeit oder Integrität der Daten wichtige Gesichtspunkte darstellen, sollten Verschlüsselungsverfahren zum Schutz der Daten auf Wechselmedien angewendet werden;
- e) Um das Risiko des Verlusts noch benötigter Daten aufgrund von Medienalterung zu mindern, sollten die Daten auf neue Datenträger umgespeichert werden, bevor diese unlesbar werden;
- f) Von besonders wichtigen Daten sollten Kopien auf separaten Datenträgern erstellt werden, um das Risiko eines Datenfehlers oder -verlusts weiter zu verringern;
- g) Zur Begrenzung der Gefahr eines Datenverlusts sollte eine Registrierung der Wechselmedien in Betracht gezogen werden;
- h) Die Verwendung von Wechsellaufwerken sollte nur dann ermöglicht werden, wenn es dafür geschäftliche Gründe gibt;
- i) Falls eine Notwendigkeit zur Verwendung von Wechseldatenträgern besteht, sollte die Übertragung von Daten auf diese Medien überwacht werden.

Verfahren und Berechtigungsebenen sollten dokumentiert werden.

8.3.2 Entsorgung von Medien

Maßnahme

Datenträger sollten sicher und unter Anwendung formeller Verfahrensanweisungen entsorgt werden, wenn sie nicht mehr benötigt werden.

Umsetzungshinweise

Es sollten formelle Verfahrensweisen zur sicheren Entsorgung von Medien festgelegt werden, um das Risiko einer Offenlegung von Informationen gegenüber nicht autorisierten Personen möglichst gering zu halten. Die Verfahrensweisen zur sicheren Entsorgung von Medien, die vertrauliche Informationen enthalten, sollten der Sensibilität dieser Daten Rechnung tragen. Die folgenden Punkte sollten dabei berücksichtigt werden:

- a) Medien, die vertrauliche Daten enthalten, sollten sicher gelagert und sicher entsorgt werden, z. B. durch Verbrennung oder Schreddern oder durch Löschung der Daten mittels einer anderen Anwendung innerhalb der Organisation;
- b) Es sollten Verfahren zur Ermittlung von Daten existieren, bei denen eine derartige Entsorgung erforderlich ist;
- c) Es kann einfacher sein, sämtliche Datenträger zu sammeln und sicher zu entsorgen, statt eine Einzelbestimmung der Medien vorzunehmen, die tatsächlich sensible Daten enthalten;
- d) Viele Organisationen bieten die Sammlung und Beseitigung von Medien an. Die Auswahl eines geeigneten externen Dienstleisters sollte mit Bedacht und unter der Voraussetzung erfolgen, dass dieser angemessene Sicherheitsmaßnahmen und Erfahrung vorweisen kann;
- e) Die Entsorgung von Medien mit sensiblen Daten sollte protokolliert werden, um einem Prüfpfad zu entsprechen.

Bei der Sammlung zur Entsorgung bestimmter Medien sollte auf den Kumulierungseffekt geachtet werden, durch den eine große Menge nicht sensibler Informationen zusammengekommen einen Bestand sensibler Daten darstellen kann.

Weitere Informationen

Beschädigte Datenträger, die sensible Daten enthalten, müssen möglicherweise einer Risikoeinschätzung unterzogen werden, um zu bestimmen, ob diese Medien physisch zerstört, zur Reparatur versandt oder anderweitig ausgesondert werden sollten.

8.3.3 Transport physischer Medien

Maßnahme

Medien, auf denen Informationen gespeichert sind, sollten vor unautorisiertem Zugriff, missbräuchlicher Verwendung oder Verfälschung während des Transports geschützt werden.

Umsetzungshinweise

Die folgenden Leitlinien sollten berücksichtigt werden, um Medien zu schützen, auf denen Informationen transportiert werden:

- a) Es sollten zuverlässige Transport- bzw. Kurierdienstleister beauftragt werden;
- b) Mit dem Management sollte eine Liste autorisierter Kurierdienste vereinbart werden;
- c) Es sollten Verfahren entwickelt werden, um die Identität der Kuriere sicher festzustellen;

- d) Die Verpackung sollte ausreichend sein, um den Schutz des Inhalts vor physischen Beschädigungen zu schützen, zu denen es während des Transports kommen kann, und den Spezifikationen des Herstellers entsprechen, zum Beispiel was den Schutz vor Umweltfaktoren wie Hitze, Feuchtigkeit oder elektromagnetische Felder betrifft, die die Wiederherstellungsfähigkeit der Medien herabsetzen kann;
- e) Es sollten Protokolle geführt werden, aus denen der Inhalt der Medien, die angewendeten Schutzmaßnahmen sowie die Transferzeiten zu den Transportwächtern und die Entgegennahme am Bestimmungsort hervorgehen.

Weitere Informationen

Daten können einem unberechtigten Zugriff, einer Fehlanwendung oder einer Verfälschung während des Transports ausgesetzt sein, wenn Medien z. B. über einen Postdienstleister oder per Kurier versandt werden. Im Rahmen dieser Maßnahme gehören zu den Medien auch Papierdokumente.

Wenn die vertraulichen Informationen auf den Medien nicht verschlüsselt sind, sollte eine zusätzliche physische Sicherung der Medien in Betracht gezogen werden.

9 Zugriffskontrolle

9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle

Zielsetzung: Beschränkung des Zugriffs auf Informationen und informationsverarbeitende Einrichtungen.

9.1.1 Leitlinie zur Zugangskontrolle

Maßnahme

Eine Leitlinie zur Zugangskontrolle sollte auf Grundlage der geschäftlichen und der die Informationssicherheit betreffenden Anforderungen erstellt, dokumentiert und geprüft werden.

Umsetzungshinweise

Werteeigentümer sollten entsprechende Zugangskontrollregeln, Zugangsrechte und -beschränkungen für bestimmte Benutzerfunktionen in Bezug auf ihre Werte bestimmen, und zwar mit einer Detailliertheit und Strenge, die den Sicherheitsrisiken im Zusammenhang mit den betreffenden Informationen gerecht wird.

Zugangskontrollen sollten sowohl logischer als auch physischer Natur sein (siehe 11) und gemeinsam geplant werden. Benutzern und Dienstleistern sollten die geschäftlichen Anforderungen, die diese Zugangskontrollen erfüllen sollen, klar vor Augen geführt werden.

In der Richtlinie sollten die folgenden Punkte Berücksichtigung finden:

- a) Sicherheitsanforderungen von Geschäftsanwendungen;
- b) Richtlinien zur Verteilung von Informationen und zur Genehmigung des Zugriffs auf diese, z. B. der Grundsatz „Kenntnis nur wenn erforderlich“, Informationssicherheitsstufen und Klassifizierung von Informationen (siehe 8.2);
- c) Konsistenz zwischen den Zugangsberechtigungen und den Richtlinien zur Klassifizierung von Informationen in verschiedenen Systemen und Netzen;
- d) Relevante Gesetzgebung und vertragliche Verpflichtungen hinsichtlich der Begrenzung des Zugriffs auf Daten oder Dienstleistungen (siehe 18.1);
- e) Verwaltung von Zugangsrechten in einer verteilten und vernetzten Umgebung, die alle verfügbaren Verbindungsarten anerkennt;

- f) Trennung der Zugangskontrollregeln, z. B. Zugangsbeantragung, Zugangsgenehmigung, Zugangsverwaltung;
- g) Anforderungen für die offizielle Genehmigung von Zugangsbeantragungen (siehe 9.2.1);
- h) Anforderungen für die regelmäßige Überprüfung von Zugangsberechtigungen (siehe 9.2.5);
- i) Entziehung von Zugangsrechten (siehe 9.2.6);
- j) Archivierung der Aufzeichnungen aller signifikanten Ereignisse bezüglich der Nutzung und Verwaltung von Benutzeridentitäten und geheimen Authentisierungsinformationen;
- k) Funktionsträger mit privilegiertem Zugang (siehe 9.2.3).

Weitere Informationen

Bei der Festlegung der zu beachtenden Zugangskontrollregeln sollte mit besonderer Sorgfalt vorgegangen werden. Dabei sind folgende Punkte zu beachten:

- a) Festlegung von Regeln auf Grundlage der Prämisse, dass grundsätzlich alles verboten ist, was nicht ausdrücklich gestattet wird (und nicht umgekehrt);
- b) automatisch durch Einrichtungen zur Informationsverarbeitung bzw. durch einen Benutzer vorgenommene Änderungen bei der Kennzeichnung von Informationen (siehe 8.2.2);
- c) automatisch durch das Informationssystem bzw. durch einen Administrator vorgenommene Änderungen von Benutzerbefugnissen;
- d) Regeln, für deren Inkrafttreten eine Genehmigung erforderlich bzw. nicht erforderlich ist.

Zugangskontrollregeln sollten durch formelle Verfahrensweisen (siehe 9.2, 9.3, 9.4) und festgelegte Verantwortlichkeiten (siehe 6.1.1, 9.2, 15.1) unterstützt werden.

Funktionsbasierte Zugangskontrollen sind ein von vielen Organisationen erfolgreich genutzter Ansatz zur Verknüpfung von Zugangsrechten mit Geschäftsfunktionen.

Zwei der häufigsten Prinzipien, die die Leitlinie zur Zugangskontrolle bestimmen, sind:

- a) Kenntnis nur wenn nötig: Man erhält nur Zugang zu Informationen, die zur Ausführung der eigenen Aufgaben benötigt werden (unterschiedliche Aufgaben/Funktionen bedeuten unterschiedliche Berechtigungen und damit ein unterschiedliches Zugangsprofil);
- b) Nutzung nur wenn nötig: Man erhält nur Zugang zu den Einrichtungen zur Informationsverarbeitung (IT-Ausrüstung, Anwendungen, Verfahren, Räume), die zur Ausführung der eigenen Aufgaben/ Tätigkeiten/ Funktionen benötigt werden.

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Maßnahme

Benutzer sollten ausschließlich zu denjenigen Netzwerken und Netzwerkdiensten Zugang erhalten, zu deren Nutzung sie ausdrücklich autorisiert wurden.

Umsetzungshinweise

Es sollte eine Richtlinie zur Nutzung von Netzwerken und Netzwerkdiensten formuliert werden. Diese Richtlinie sollte folgende Punkte umfassen: