

DIN ISO/IEC 27002

ICS 03.100.70; 35.030

Ersatz für
DIN ISO/IEC 27002:2008-09**Informationstechnologie –
IT-Sicherheitsverfahren –
Leitfaden für Informationssicherheits-Maßnahmen (ISO/IEC 27002:2013 +
Cor. 1:2014 + Cor. 2:2015)**

Information technology –
Security techniques –
Code of practice for information security controls (ISO/IEC 27002:2013 + Cor. 1:2014 +
Cor. 2:2015)

Technologies de l'information –
Techniques de sécurité –
Code de bonne pratique pour le management de la sécurité de l'information
(ISO/CEI 27002:2013 + Cor. 1:2014 + Cor. 2:2015)

Gesamtumfang 106 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
0 Einleitung	6
1 Anwendungsbereich.....	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Aufbau dieser Norm.....	9
4.1 Abschnitte.....	9
4.2 Maßnahmenkategorien.....	9
5 Informationssicherheitsrichtlinien.....	10
5.1 Vorgaben der Leitung für 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 Beschäftigung.....	18
7.2 Während der Beschäftigung	20
7.3 Beendigung und Änderung der Beschäftigung	23
8 Verwaltung der Werte	23
8.1 Verantwortlichkeit für Werte	23
8.2 Informationsklassifizierung.....	26
8.3 Handhabung von Datenträgern.....	28
9 Zugangssteuerung	30
9.1 Geschäftsanforderungen an die Zugangsteuerung	30
9.2 Benutzerzugangsverwaltung	33
9.3 Benutzerverantwortlichkeiten.....	37
9.4 Zugangssteuerung für Systeme und Anwendungen.....	38
10 Kryptographie.....	42
10.1 Kryptographische Maßnahmen.....	42
11 Physische und umgebungsbezogene Sicherheit.....	45
11.1 Sicherheitsbereiche.....	45
11.2 Geräte und Betriebsmittel.....	49
12 Betriebssicherheit.....	55
12.1 Betriebsabläufe und -verantwortlichkeiten	55
12.2 Schutz vor Schadsoftware.....	58
12.3 Datensicherung	60
12.4 Protokollierung und Überwachung.....	61
12.5 Steuerung von Software im Betrieb.....	63
12.6 Handhabung technischer Schwachstellen.....	65
12.7 Audits von Informationssystemen	67
13 Kommunikationssicherheit.....	67

13.1	Netzwerksicherheitsmanagement.....	67
13.2	Informationsübertragung	70
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	74
14.1	Sicherheitsanforderungen an Informationssysteme	74
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	77
14.3	Testdaten.....	83
15	Lieferantenbeziehungen.....	84
15.1	Informationssicherheit in Lieferantenbeziehungen	84
15.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	88
16	Handhabung von Informationssicherheitsvorfällen.....	90
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	90
17	Informationssicherheitsaspekte beim Business Continuity Management	95
17.1	Aufrechterhalten der Informationssicherheit.....	95
17.2	Redundanzen	97
18	Compliance	98
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen.....	98
18.2	Überprüfungen der Informationssicherheit	102
	Literaturhinweise.....	105

Nationales Vorwort

Die Internationale Norm ISO/IEC 27002:2013-10 + Cor. 1:2014 + Cor. 2:2015 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 deutsche Sprachfassung wurde vom DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) in Zusammenarbeit mit der Schweizerischen Normenvereinigung (SNV) erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Der Beginn und das Ende des vom Corrigendum 1 und Corrigendum 2 geänderten Textes werden durch die Markierungen **A1** **A1** sowie **A2** **A2** angezeigt.

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

Frühere Ausgaben

DIN ISO/IEC 27002: 2008-09

Nationaler Anhang NA (informativ)

Literaturhinweise

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

Informationstechnologie — IT-Sicherheitsverfahren — Leitfaden für Informationssicherheits-Maßnahmen (ISO/IEC 27002:2013 + Cor.1:2014 + Cor.2:2015)

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 [10] 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, die deren spezifisches Umfeld der Informationssicherheitsrisiken berücksichtigen.

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 Unternehmenswerte für die Geschäftsziele einer Organisation wichtig sind, und damit einen Schutz gegen unterschiedliche Gefährdungen verdienen oder erfordern.

Organisationseigene Werte unterliegen sowohl vorsätzlichen als auch unbeabsichtigten 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, sind Risiken in der Informationssicherheit daher immer allgegenwärtig. 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 [10] näher beschrieben, verfolgt eine ganzheitliche, koordinierte Betrachtung der Risiken in der Informationssicherheit eines Unternehmens, um eine umfassende Sammlung 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 [10] und dieser Norm als sicher betrachtet werden können. Die Sicherheit mithilfe technischer Mittel ist begrenzt und sollte mit geeignetem Führungsverhalten und Verfahren unterstützt werden. Die Feststellung der benötigten Sicherheitsmaßnahmen erfordert sorgfältige Planung und Detailtreue. Ein erfolgreiches Informationssicherheits-Managementsystem erfordert die Mitarbeit aller Beschäftigten einer Organisation. Die Organisation benötigt unter Umständen auch die Mitwirkung von Gesellschaftern, Lieferanten und anderen externen Parteien. Fachliche Beratung durch externe Parteien 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 identifiziert. Es existieren drei Hauptquellen für Sicherheitsanforderungen:

- a) die Beurteilung von Risiken für die Organisation unter Berücksichtigung der Unternehmensstrategie und der Geschäftsziele. Mithilfe einer Risikobewertung können Bedrohungen der organisationseigenen Werte identifiziert, Anfälligkeit und Eintrittswahrscheinlichkeit bewertet und mögliche Auswirkungen geschätzt werden;
- b) die rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen, die eine Organisation, seine Handelspartner, Auftragnehmer und Dienstleister erfüllen müssen sowie deren soziokulturelles Umfeld;
- c) eine Reihe von Grundsätzen, Zielen und Geschäftsanforderungen, 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 potenziellen Unternehmensschaden abgewogen werden, der wahrscheinlich bei Fehlen dieser Maßnahmen 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 [11] bietet eine Anleitung zum Management von Informationssicherheitsrisiken, einschließlich Empfehlungen zu Bewertung, Behandlung, Akzeptanz, Kommunikation, Überwachung und Prüfung von Risiken.

0.3 Auswahl von Maßnahmen

Maßnahmen können entweder dieser Norm oder anderen Maßnahmensammlungen entnommen werden. Auch neue Maßnahmen können entwickelt werden, um gegebenenfalls spezifische Anforderungen zu erfüllen.

Die Auswahl der Maßnahmen 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 Maßnahmen hängt ebenfalls von der Art und Weise ab, wie Maßnahmen interagieren, um gestaffelte Sicherheitsebenen bereitstellen zu können.

Einige der Maßnahmen in dieser Norm können als Richtlinien für das Management für Informationssicherheit betrachtet werden und sind in den meisten Organisationen anwendbar. Die Maßnahmen werden im Folgenden zusammen mit Umsetzungshinweisen näher erläutert. Weitere Informationen zur Auswahl von Maßnahmen und anderen Risikobehandlungsmöglichkeiten sind in ISO/IEC 27005 [11] verfügbar.

0.4 Entwicklung eigener Leitfäden

Diese Internationale Norm kann als Ausgangspunkt für die Entwicklung organisationsspezifischer Leitfäden angesehen werden. Möglicherweise sind nicht alle der in diesem Leitfaden angegebenen Maßnahmen und Orientierungshilfen anwendbar. Darüber hinaus könnten zusätzliche, nicht hier aufgeführte Maßnahmen

und Leitfäden erforderlich sein. Bei der Verfassung von Dokumenten mit zusätzlichen Richtlinien oder Maßnahmen kann es sinnvoll sein, gegebenenfalls Querverweise auf Abschnitte in dieser Norm anzugeben, um Einhaltungsprüfungen durch Auditoren 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 zur möglichen Vernichtung 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, umgesetzt, genutzt, gepflegt und schließlich ausgemustert und entsorgt 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 diese Norm als Orientierung 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 den Anwendungsbereich und die Ziele einzelner Normen.

1 Anwendungsbereich

Diese Internationale Norm enthält Leitfäden für organisatorische Normen und Managementpraktiken bezüglich Informationssicherheit, einschließlich Auswahl, Umsetzung und Handhabung von Maßnahmen unter Berücksichtigung der Umgebung 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 [10] auszuwählen;
- b) allgemein akzeptierte Maßnahmen für Informationssicherheit umzusetzen;
- c) ihre eigenen Richtlinien eines Managements für Informationssicherheit zu entwickeln.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung des Dokuments erforderlich. Bei datierten Verweisungen 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 Hauptsicherheitskategorien und 114 Maßnahmen.

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 allen Kategorien wichtig sein. Daher sollte jede Organisation, die diese Norm anwenden möchte, für sie zutreffende Maßnahmen identifizieren und feststellen, wie wichtig sie sind und inwieweit sie auf einzelne Geschäftsprozesse anwendbar sind. Darüber hinaus sind Listen in dieser Norm nicht in der Reihenfolge ihrer Priorität geordnet.

4.2 Maßnahmenkategorien

Jede Hauptmaßnahmenkategorie enthält:

- a) Ein Maßnahmenziel, das angibt, was erreicht werden soll;
- b) eine oder mehrere Maßnahme(n), die zur Erreichung des Maßnahmenzieles angewendet werden kann.

Die Beschreibungen der Maßnahmen sind wie folgt strukturiert:

Maßnahme

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

Anleitung zur Umsetzung

Bietet detaillierte Information zur Umsetzung von Maßnahmen um das jeweilige Maßnahmenziel zu erreichen. Die Hinweise sind vielleicht nicht in allen Situationen ausreichend oder könnten nur eingeschränkt anwendbar sein und erfüllen möglicherweise nicht die spezifische Maßnahmenanforderung einer Organisation.

Weitere Informationen

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

5 Informationssicherheitsrichtlinien

5.1 Vorgaben der Leitung für Informationssicherheit

Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.

5.1.1 Informationssicherheitsrichtlinien

Maßnahme

Ein Satz Informationssicherheitsrichtlinien sollte festgelegt sein, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.

Anleitung zur Umsetzung

Organisationen sollten auf höchster Ebene eine „Informationssicherheitspolitik“^{N1)} definieren, die vom Management genehmigt ist und einen Ansatz zur Bewältigung der Informationssicherheitsziele festlegt.

Richtlinien zur Informationssicherheit sollten Anforderungen behandeln, die entstehen durch:

- a) Geschäftsstrategie;
- b) Vorschriften, Gesetze und Verträge;
- c) das aktuelle und voraussichtliche Bedrohungsumfeld der Informationssicherheit.

Die Informationssicherheitspolitik sollte Aussagen enthalten über:

- a) Die Definition von Informationssicherheit, Zielen und Grundsätzen, um alle Aktivitäten in Bezug auf Informationssicherheit lenken zu können;
- b) Zuordnung allgemeiner und spezifischer Verantwortlichkeiten zu definierten Rollen für die Handhabung von Informationssicherheit;
- c) Prozesse für den Umgang mit Abweichungen und Ausnahmen.

N1) Nationale Fußnote: Die Richtlinie auf höchster Ebene wird gemäß DIN ISO/IEC 27001 als Politik bezeichnet.

Auf tieferer Ebene sollte die Informationssicherheitspolitik durch themenspezifische Richtlinien unterstützt werden, die zusätzlich die Umsetzung von Maßnahmen zur Informationssicherheit anordnen. Diese Richtlinien 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) Zugangssteuerung (siehe Abschnitt 9);
- b) Informationsklassifizierung (und deren Handhabung) (siehe 8.2);
- c) physische und umgebungsbezogene Sicherheit (siehe Abschnitt 11);
- d) an den Endanwender gerichtete Themen wie:
 - 1) zulässiger Gebrauch von Werten (siehe 8.1.3);
 - 2) Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren (siehe 11.2.9);
 - 3) Informationsübertragung (siehe 13.2.1);
 - 4) Mobilgeräte und Telearbeit (siehe 6.2);
 - 5) Einschränkung von Softwareinstallationen und -verwendung (siehe 12.6.2);
- e) Datensicherung (siehe 12.3);
- f) Informationsübertragung (siehe 13.2);
- g) Schutz vor Schadsoftware (siehe 12.2);
- h) Handhabung technischer Schwachstellen (siehe 12.6.1);
- i) kryptographische Maßnahmen (siehe Abschnitt 10);
- j) Kommunikationssicherheit (siehe Abschnitt 13);
- k) Privatsphäre und Schutz von personenbezogener Information (siehe 18.1.4);
- l) Lieferantenbeziehungen (siehe Abschnitt 15).

Diese Richtlinien sollten Beschäftigten und allen maßgeblichen externen Parteien in einer Form kommuniziert werden, die für die Zielgruppe relevant, zugänglich und verständlich ist, z. B. im Kontext eines Programms für die „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ (siehe 7.2.2).

Weitere Informationen

Der Bedarf an internen Richtlinien zur Informationssicherheit variiert je nach Organisation. Interne Richtlinien sind besonders nützlich in größeren, komplexeren Organisationen, in denen die Stellen, die zu erreichende Ausprägungen von Maßnahmen festlegen und genehmigen, von den Stellen getrennt sind, die diese Maßnahmen einführen, oder wo eine Richtlinie für eine Vielzahl von Personen oder Funktionen einer Organisation gilt. Richtlinien für Informationssicherheit können in einer einzelnen „Richtlinie zur Informationssicherheit“ oder in mehreren einzelnen, aber zusammengehörigen Dokumenten verfasst werden.

Falls Richtlinien für Informationssicherheit außerhalb der Organisation verbreitet werden, sollte darauf geachtet werden, dass keine vertraulichen Informationen veröffentlicht werden.

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

5.1.2 Überprüfung der Informationssicherheitsrichtlinien

Maßnahme

Die Informationssicherheitsrichtlinien sollten in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

Anleitung zur Umsetzung

Jede Richtlinie sollte einen Zuständigen haben, dem die Handhabungsverantwortung für Entwicklung, Überprüfung und Bewertung der Richtlinien übertragen wurde. Die Überprüfung sollte eine Bewertung des Verbesserungspotenzials für Richtlinien der Organisation enthalten und einen Ansatz zur Handhabung von Informationssicherheit umfassen, als Reaktion auf Änderungen im organisatorischen Umfeld, der geschäftlichen und gesetzlichen Rahmenbedingungen und der technischen Umgebung.

Die Überprüfung der Richtlinien zur Informationssicherheit sollte die Ergebnisse der Managementbewertung berücksichtigen.

Eine überarbeitete Richtlinie sollte durch das Management genehmigt werden.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.

6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Maßnahme

Alle Informationssicherheitsverantwortlichkeiten sollten festgelegt und zugeordnet sein.

Anleitung zur Umsetzung

Verantwortlichkeiten für Informationssicherheit sollten in Übereinstimmung mit den Richtlinien zur Informationssicherheit zugeordnet werden (siehe 5.1.1). Verantwortungen zum Schutz individueller Werte und zum Ausführen spezifischer Informationssicherheitsprozesse sollten identifiziert werden. Verantwortlichkeiten für Informationssicherheitsrisikomanagementtätigkeiten und insbesondere für die Akzeptanz von Restrisiken sollten definiert werden. Diese Verantwortlichkeiten sollten soweit erforderlich um detaillierte Anleitungen für bestimmte Standorte und Einrichtungen der Informationsverarbeitung erweitert werden. Lokale Verantwortungen für den Schutz von Werten und für das Ausführen spezifischer Sicherheitsprozesse sollten definiert werden.

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

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

- a) Werte und Informationssicherheitsprozesse sollten identifiziert und definiert werden;

- b) die verantwortliche Entität für jeden Wert oder Informationssicherheitsprozess sollte zugeordnet 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 die ernannten Personen in diesem Bereich kompetent sein und die Gelegenheit erhalten, mit Entwicklungen Schritt halten zu können;
- e) Koordination der und Überblick über die Informationssicherheitsaspekte in Lieferantenbeziehungen sollten identifiziert und dokumentiert werden.

Weitere Informationen

Viele Organisationen ernennen einen Manager für Informationssicherheit, der die Gesamtverantwortung für Entwicklung und Umsetzung der Informationssicherheit übernimmt und die Identifizierung von Maßnahmen unterstützt.

Allerdings verbleibt die Verantwortung für die Bereitstellung von Mitteln und Umsetzung von Maßnahmen oft bei den einzelnen Managern. Eine gängige Praxis ist es, einen Eigentümer für jeden Wert zu ernennen, der dann für den laufenden Schutz der Werte verantwortlich ist.

6.1.2 Aufgabentrennung

Maßnahme

Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sollten getrennt werden, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.

Anleitung zur Umsetzung

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

Für kleine Organisationen könnte Aufgabentrennung nur mit Schwierigkeiten zu erreichen sein, das Prinzip sollte aber so weit wie möglich und praktikabel angewandt 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 mit Behörden

Maßnahme

Angemessene Kontakte mit relevanten Behörden sollten gepflegt werden.

Anleitung zur Umsetzung

Organisationen sollten über Verfahren verfügen, die festlegen, wann und durch wen 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, benötigen möglicherweise Behörden, um Schritte gegen die Angriffsquelle zu ergreifen.

Die Pflege solcher Kontakte könnte eine Anforderung für die Unterstützung bei Informationssicherheitsvorfällen (siehe Abschnitt 16) oder für den Business Continuity und Notfallplanungsprozess (siehe Abschnitt 17) sein. Kontakte mit Aufsichtsbehörden helfen auch bei der Vorwegnahme und Vorbereitung anstehender Änderungen von Gesetzen oder Regulierungen, die von der Organisation umgesetzt werden müssen. Kontakte mit anderen Behörden umfassen auch Versorgungseinrichtungen, wie Notdienste, Stromversorgungsunternehmen, Hilfs- und Rettungsdienste z. B. Feuerwehr (in Verbindung mit Business Continuity), Telekommunikationsanbieter (in Verbindung mit Leitungsverlegung und Verfügbarkeit) und Wasserversorger (in Verbindung mit Kühleinrichtungen für Geräte).

6.1.4 Kontakt mit speziellen Interessensgruppen

Maßnahme

Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden sollten gepflegt werden.

Anleitung zur Umsetzung

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

- a) die Kenntnis über beste Praktiken zu verbessern und über relevante Sicherheitsinformationen auf dem Laufenden zu bleiben;
- b) sicherzustellen, dass das Verständnis im Umfeld der Informationssicherheit aktuell und vollständig ist;
- c) um rechtzeitig Warnungen, Hinweise und Patches 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 Abschnitt 16).

Weitere Informationen

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

6.1.5 Informationssicherheit im Projektmanagement

Maßnahme

Informationssicherheit sollte im Projektmanagement berücksichtigt werden, ungeachtet der Art des Projekts.

Anleitung zur Umsetzung

Informationssicherheit sollte in die Projektmanagementmethode(n) einer Organisation integriert werden, damit Informationssicherheitsrisiken 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) Informationssicherheitsziele in den Projektzielen enthalten sind;
- b) eine Informationssicherheitsrisikobeurteilung in einem frühen Stadium des Projektes durchgeführt wird, um notwendige Maßnahmen zu identifizieren;
- c) Informationssicherheit Bestandteil aller Phasen der angewandten 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 Rollen zugewiesen werden.

6.2 Mobilgeräte^{N2)} und Telearbeit

Ziel: Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.

6.2.1 Richtlinie zu Mobilgeräten

Maßnahme

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sollten umgesetzt werden, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.

Anleitung zur Umsetzung

Bei der Verwendung von Mobilgeräten sollte besonders darauf geachtet werden, dass Geschäftsinformationen nicht beeinträchtigt werden. Die Richtlinie für Mobilgeräte sollte die Risiken im Umgang mit Mobilgeräten in ungeschützten Umgebungen berücksichtigen.

Die Richtlinie für Mobilgeräte sollte berücksichtigen:

- a) Registrierung von Mobilgeräten;
- b) Anforderungen für den physischen Schutz;
- c) Einschränkung von Software-Installation;
- d) Anforderungen an Software-Versionen der Mobilgeräte und Anwendung von Patches;

N2) Nationale Fußnote: Mobilgeräte umfassen mobile Geräte jeder Art (Smartphones, Tablets, Laptops, Netbooks, usw.)

- e) Verbindungseinschränkungen zu Informationsdiensten;
- f) Maßnahmen zum Zugang zu Mobilgeräten;
- g) Verschlüsselungsverfahren;
- h) Schutz vor Schadsoftware;
- i) Remote-Deaktivierung, Löschung oder Sperrung;
- j) Backups;
- k) Nutzung von Web-Diensten und Web-Anwendungen.

Bei der Verwendung von Mobilgeräten an öffentlichen Plätzen, in Besprechungsräumen 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 Abschnitt 10) und zwingende Anwendung geheimer Authentifizierungsdaten (siehe 9.2.4).

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 die wichtige, sensible oder geschäftskritische Geschäftsinformation beinhalten, sollten nicht unbeaufsichtigt gelassen und wenn möglich unter Verschluss gehalten oder mit Spezialschlössern gesichert werden.

Für das Personal, welches Mobilgeräte benutzt, sollten Schulungen angeboten werden, um ihr Bewusstsein für die zusätzlichen Risiken, die aus dieser Arbeitsweise resultieren und für die Maßnahmen, die umgesetzt werden sollten, zu schärfen.

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

- a) Trennung von privater und geschäftlicher Nutzung der Geräte, einschließlich Software zur 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, etc.), ihren Verzicht auf das Eigentum von Geschäftsdaten erklären und der Organisation im Fall des Diebstahls oder Verlusts des Gerätes oder bei Wegfall der Befugnis zur Dienstbenutzung das Löschen der Daten per Fernzugriff zu erlauben. Diese Richtlinie 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 Maßnahmen 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. Netzwerkfunktion, Internetzugang, E-Mail-Zugriff und Dateioperationen. Informationssicherheitsmaßnahmen für Mobilgeräte bestehen in der Regel aus Maßnahmen, die für ortsfeste Geräte eingeführt wurden und solchen, um die Bedrohungen durch die Verwendung außerhalb der Räumlichkeiten der Organisation zu adressieren.

6.2.2 Telearbeit

Maßnahme

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sollten umgesetzt sein.

Anleitung zur Umsetzung

Organisationen, die Telearbeit erlauben, sollten eine Richtlinie zur Definition von Bedingungen und Einschränkungen für die Nutzung von Telearbeit erlassen. Soweit erforderlich und gesetzlich zulässig, sollten folgende Themen 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 Information auf die zugegriffen und die über Telekommunikationsverbindungen weitergegeben wird sowie die Empfindlichkeit der internen Systeme;
- d) die Bereitstellung von virtuellen Desktop-Zugriffen, der Verarbeitung und Speicherung von Information auf privaten Geräten unterbindet;
- e) die Gefahr des unbefugten Zugriffs auf Information durch andere Personen in derselben Unterkunft, 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 Geräten in Privateigentum (um die Sicherheit der Maschine zu überprüfen oder während einer Untersuchung), der von Gesetzes wegen verhindert werden könnte;
- i) Software-Lizenzvereinbarungen, die dergestalt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Arbeitsgeräten von Beschäftigten oder sonstiger Benutzer, die zu externen Parteien gehören verantwortlich werden könnten;
- j) Anforderungen an Schadsoftwareschutz und Firewall.

Die zu berücksichtigen Richtlinien und Regelungen sollten enthalten:

- a) die Bereitstellung geeigneter Geräte und Aufbewahrungsmöbel für Telearbeitstätigkeiten, dort wo der Einsatz von privaten, nicht unter der Aufsicht der Organisation stehenden Geräten untersagt ist;

- b) die Festlegung gestatteter Arbeit, die Arbeitszeit, die Klassifizierung aufbewahrter Informationen und die internen Systeme und Dienste, auf die der Telearbeiter berechtigten Zugriff hat;
- c) die Bereitstellung geeigneter Telekommunikationseinrichtungen, einschließlich Methoden zur Sicherung des Fernzugriffs;
- d) physische Sicherheit;
- e) Regeln und Leitfäden für den Zugang von Familie und Besuchern zu Geräten und Informationen;
- f) die Bereitstellung von Hard- und Software Support und Wartung;
- g) Bereitstellung von Versicherungen;
- h) Verfahren für Backups und Business Continuity;
- i) Auditierung und Überwachung der Sicherheit;
- j) Widerruf von Befugnissen und Zugriffsrechten sowie die Rückgabe von Geräten wenn die Telearbeits-tätigkeiten beendet sind.

Weitere Informationen

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

7 Personalsicherheit

7.1 Vor der Beschäftigung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.

7.1.1 Sicherheitsüberprüfung

Maßnahme

Alle Personen, die sich um eine Beschäftigung bewerben, sollten einer Sicherheitsüberprüfung unterzogen werden, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.

Anleitung zur Umsetzung

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

- a) Vorhandensein zufriedenstellender Leumundszeugnisse, z. B. ein dienstliches und ein persönliches Zeugnis;
- b) ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers;
- 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 Rolle 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 Rolle 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 Informationen, sollte die Organisation weitere, eingehendere Überprüfungen in Betracht ziehen.

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

Auch für Auftragnehmer sollte ein Überprüfungsverfahren sichergestellt 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 Bewerber, die für Positionen in der Organisation infrage kommen, sollten im Einvernehmen mit entsprechenden Gesetzen in der jeweiligen Rechtsordnung gesammelt und verarbeitet werden. Je nach geltender Rechtsvorschrift sollten die Bewerber im Voraus über Überprüfungstätigkeiten informiert werden.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Maßnahme

In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sollten deren Verantwortlichkeiten und diejenigen der Organisation festgelegt werden.

Anleitung zur Umsetzung

Die Arbeitsvertragsklauseln sollten die Informationssicherheitsrichtlinien der Organisation widerspiegeln, und außerdem die folgenden Punkte verdeutlichen und festhalten:

- a) dass alle Beschäftigten und Auftragnehmer, die Zugang zu vertraulichen Informationen erhalten, eine Vertraulichkeitserklärung oder Geheimhaltungsvereinbarung unterzeichnen sollten, bevor sie Zugang zu Einrichtungen zur Informationsverarbeitung erhalten (siehe 13.2.4);
- b) gesetzliche Verantwortlichkeiten und Rechte der Beschäftigten oder Auftragnehmer, z. B. bezüglich Urheberrechtsgesetzen oder Datenschutzgesetzgebung (siehe 18.1.2 und 18.1.4);
- c) Verantwortungen für die Klassifizierung von Informationen und die Verwaltung organisationseigener **[A₁]** Information und anderer **[A₁]** Werte, die mit Informationen, Einrichtungen zur Informationsverarbeitung und Informationsdiensten assoziiert sind, die von Beschäftigten und Auftragnehmern verarbeitet werden (siehe Abschnitt 8);
- d) Verantwortlichkeiten der Beschäftigte oder Auftragnehmer für den Umgang mit Informationen, die von anderen Unternehmen oder externen Parteien stammen;
- e) Maßnahmen, die ergriffen werden müssen, falls die Beschäftigten 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 Beschäftigte 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 Verantwortlichkeiten für Informationssicherheit der Beschäftigten und Auftragnehmer in Bezug auf Geheimhaltung, Datenschutz, ethische Grundsätze, angemessene Nutzung von Betriebsmitteln und Einrichtungen sowie von der Organisation erwartete, seriöse Praktiken anzugeben. Von einer externen Partei, mit der ein Auftragnehmer assoziiert ist, kann verlangt werden, eine Vereinbarung im Namen der verpflichteten Person einzugehen.

7.2 Während der Beschäftigung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten bezüglich der Informationssicherheit bewusst sind und diesen nachkommen.

7.2.1 Verantwortlichkeiten der Leitung

Maßnahme

Die Leitung sollte von allen Beschäftigten und Auftragnehmern verlangen, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.

Anleitung zur Umsetzung

Die Verantwortlichkeiten der Leitung sollten unter anderem beinhalten, dass Beschäftigte und Auftragnehmer:

- a) über ihre Rollen und Verantwortlichkeiten in der Informationssicherheit informiert werden bevor sie Zugang zu vertraulicher Information und Informationssystemen erhalten;
- b) Leitfäden erhalten, die die Erwartungen an ihre Rolle in der Informationssicherheit innerhalb der Organisation darlegen;
- c) motiviert sind, den Richtlinien für Informationssicherheit der Organisation gerecht zu werden;
- d) ein Informationssicherheitsbewußtsein erreichen, das ihren Rollen und Verantwortlichkeiten in der Organisation entspricht (siehe 7.2.2);
- e) die Beschäftigungsbedingungen einhalten, einschließlich der Informationssicherheitspolitik der Organisation und geeigneten Arbeitsmethoden;
- f) auch in Zukunft angemessene Fähigkeiten und Qualifikationen besitzen und regelmäßig weitergebildet werden;
- g) anonym über Verletzungen von Richtlinien und Verfahren zur Informationssicherheit Bericht erstatten können („whistle blowing“).

Die Leitung sollte Richtlinien, Verfahren und Maßnahmen zur Informationssicherheit unterstützen und Vorbild sein.

Weitere Informationen

Falls sich Beschäftigte und Auftragnehmer nicht der Verantwortlichkeiten für Informationssicherheit bewusst sind, kann dies zu erheblichem Schaden für die Organisation führen. Motivierte Beschäftigte sind in der Regel zuverlässiger und verursachen weniger Informationssicherheitsvorfälle.

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

7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Maßnahme

Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, sollten ein angemessenes Bewusstsein bekommen durch Ausbildung und Schulung sowie regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.

Anleitung zur Umsetzung

Ein Sensibilisierungsprogramm für Informationssicherheit sollte darauf abzielen, dass sich Beschäftigte 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 Informations-sicherheitsrichtlinien und relevanten Verfahren der Organisation, unter Berücksichtigung der zu schützenden Information der Organisation und der schon bestehenden Maßnahmen 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 Beschäftigtenfunktionen in der Organisation und gegebenenfalls unter Berücksichtigung der organisationseigenen Erwartungen an die Sensibilisierung von Auftragnehmern geplant werden. Maßnahmen des Sensibilisierungsprogramms sollten vorher zeitlich und vorzugsweise regelmäßig eingeplant werden, damit diese Maßnahmen wiederholt werden und auch neue Beschäftigten und Auftragnehmer erfasst werden. Das Sensibilisierungsprogramm sollte regelmäßig aktualisiert werden, um in Einklang mit Richtlinien und Verfahren der Organisation zu bleiben und sollte außerdem auf gewonnenen Erkenntnissen aus Informationssicherheitsvorfällen basieren.

Sensibilisierungsschulungen sollten nach dem Sensibilisierungsprogramm für Informationssicherheit der Organisation durchgeführt werden. Sensibilisierungsschulungen können auf unterschiedlichen Wegen durchgeführt werden, darunter Klassenunterricht, Fernunterricht, Internetbasiert, Selbststudium und andere.

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

- a) Darlegung der Verpflichtung der Leitung 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 Verantwortlichkeiten zur Sicherung oder zum Schutz von Informationen, die der Organisation und externen Parteien gehören;
- d) grundsätzliche Verfahren zur Informationssicherheit (wie Berichterstattung über Informationssicherheitsvorfälle) und grundlegende Sicherheitsmaßnahmen (wie 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 Beschäftigte, die in andere 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 Richtlinien 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 Sensibilisierungsprogramms ist wichtig, nicht nur das „Was“ und „Wie“, sondern auch das „Warum“ anzusprechen. Es ist wichtig, dass Beschäftigte das Ziel der Informationssicherheit und die möglichen positiven und negativen Auswirkungen ihres Verhaltens 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.

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

7.2.3 Maßregelungsprozess

Maßnahme

Ein formal festgelegter und bekanntgegebener Maßregelungsprozess sollte eingerichtet sein, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.

Anleitung zur Umsetzung

Ein Maßregelungsprozess sollte nicht ohne vorherige Prüfung eingeleitet werden, ob tatsächlich eine Informationssicherheitsverletzung aufgetreten ist (siehe 16.1.7).

Ein formeller Maßregelungsprozess sollte eine korrekte und faire Behandlung der Beschäftigten sicherstellen, die verdächtigt werden, eine Verletzung der Informationssicherheit begangen zu haben. Ein formeller Maßregelungsprozess 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 geeignet geschult war in Bezug auf einschlägige Gesetzgebung, Geschäftsverträge und gegebenenfalls andere Faktoren.

Ein Maßregelungsprozess sollte ebenfalls zur Abschreckung verwendet werden, um Beschäftigten davon abzuhalten, Richtlinien 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 Maßregelungsprozess kann auch eine Motivation oder Ansporn werden, wenn Belohnungen für bemerkenswertes Verhalten in Bezug auf Informationssicherheit definiert sind.

7.3 Beendigung und Änderung der Beschäftigung

Ziel: Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.

7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der BeschäftigungMaßnahme

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt werden.

Anleitung zur Umsetzung

Die Mitteilung von Verantwortlichkeiten im Zusammenhang mit der Beendigung des Arbeitsverhältnisses sollte weiterhin geltende Informationssicherheitsanforderungen 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. Auftragnehmer-Verhältnisses fortgelten.

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

Änderungen bei Verantwortung oder Beschäftigung sollten genauso geregelt werden wie die Beendigung aktueller Verantwortung oder Beschäftigung, die zusammen mit dem Beginn neuer Verantwortung oder einer neuen Beschäftigung erfolgt.

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 ausgeführt.

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

8 Verwaltung der Werte**8.1 Verantwortlichkeit für Werte**

Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

8.1.1 Inventarisierung der Werte

Maßnahme

[A1] Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten erfasst und ein Inventar dieser Werte sollte erstellt und gepflegt werden. **[A1]**

Anleitung zur Umsetzung

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.

Für alle festgestellten Werte sollte ein Zuständiger benannt (siehe 8.1.2), und die Klassifizierung festgestellt werden (siehe 8.2).

Weitere Informationen

Die Inventarverzeichnisse 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 [11] bietet Beispiele von Werten, die von der Organisation bei der Ermittlung von Werten in Betracht gezogen werden könnten. Der Vorgang der Zusammenstellung eines Inventars unternehmens-eigener Werte ist eine wichtige Voraussetzung für das Risikomanagement (siehe auch ISO/IEC 27000 und ISO/IEC 27005 [11]).

8.1.2 Zuständigkeit für Werte

Maßnahme

Für alle Werte, die im Inventar geführt werden, sollte es Zuständige geben.

Anleitung zur Umsetzung

Sowohl Einzelpersonen als auch andere Entitäten mit bestätigter Verantwortung für den Lebenszyklus des Wertes können als Zuständige für Werte bestimmt werden.

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

Der Zuständige für Werte 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 Zugangskontrollrichtlinien;
- d) einen ordnungsgemäßen Umgang bei der Löschung oder Zerstörung des Wertes sicherstellen.

Weitere Informationen

Bei dem festgestellten Zuständigen kann es sich entweder um eine Person oder um eine Entität mit bestätigter Verantwortung für den kompletten Lebenszyklus eines Wertes handeln. Der identifizierte Zuständige verfügt nicht unbedingt im juristischen Sinne über Eigentumsrechte am Wert.

Routineaufgaben können delegiert werden. So kann beispielsweise ein Verwalter die Werte beaufsichtigen, die Verantwortlichkeit verbleibt jedoch beim Zuständigen.

Bei komplexen Informationssystemen kann es sinnvoll sein, Gruppen von Werten zu bestimmen, die gemeinsam einen Dienst oder eine Dienstleistung bereitstellen. In diesem Fall ist der Zuständige dieses Dienstes oder dieser Dienstleistung für deren Erbringung verantwortlich, einschließlich des Einsatzes der Werte.

8.1.3 Zulässiger Gebrauch von Werten

Maßnahme

Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten aufgestellt, dokumentiert und angewendet werden.

Anleitung zur Umsetzung

Beschäftigten und sonstigen Benutzern, die zu externen Parteien gehören, die die Werte der Organisation nutzen oder Zugang zu ihnen haben, sollten auf die Informationssicherheitsanforderungen hinsichtlich der mit Information und Einrichtungen und Ressourcen zur Informationsverarbeitung verbundenen **[A1]** Information und anderen **[A1]** Werte der Organisation hingewiesen werden. Sie sollten für ihre eigene Nutzung informationsverarbeitender Ressourcen verantwortlich sein und für jedwede derartige Nutzung, die unter ihrer Verantwortlichkeit erfolgt.

8.1.4 Rückgabe von Werten

Maßnahme

Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, sollten bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehörten, zurück geben.

Anleitung zur Umsetzung

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 Beschäftigter oder ein sonstiger Benutzer, der zu externen Parteien gehört 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 Beschäftigter oder sonstiger Benutzer, der zu externen Parteien gehört 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 Maßnahmen einrichten, um unbefugtes Kopieren relevanter Information (z.B. geistiges Eigentum) durch scheidende Beschäftigte und Auftragnehmer zu verhindern.

8.2 Informationsklassifizierung

Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.

8.2.1 Klassifizierung von Information

Maßnahme

Information sollte anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert werden.

Anleitung zur Umsetzung

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

Die Zuständigen für Informationswerte sollten für ihre Klassifizierung verantwortlich sein.

Das Klassifizierungsschema sollte Konventionen für die Klassifizierung und Kriterien zur Überprüfung der Klassifizierung nach einer gewissen Zeit beinhalten. Die Schutzstufe innerhalb des Schemas sollte mittels Analyse der Vertraulichkeits-, Integritäts- und Verfügbarkeits- sowie weiterer in Betracht gezogener Anforderungen an die Information beurteilt werden. Das Schema sollte mit der Zugangssteuerungsrichtlinie (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 innerhalb der gesamten Organisation einheitlich 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 sein, z. B. hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Die Ergebnisse der Klassifizierung sollten bei Änderungen ihres Wertes, ihrer Sensibilität und ihrer 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 erleichtert. 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 geringfügiger Verlegenheit 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 Information

Maßnahme

Ein angemessener Satz von Verfahren zur Kennzeichnung von Information sollte entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.

Anleitung zur Umsetzung

Verfahren zur Kennzeichnung von Information sollten Information selbst sowie zugehörige Werte in physischem und elektronischem Format abdecken. Die Kennzeichnung sollte dem in 8.2.1 festgelegten Klassifizierungsschema Rechnung tragen. Die Kennzeichnungen sollten einfach 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. Beschäftigten und Auftragnehmer sollten auf die Kennzeichnungsverfahren aufmerksam gemacht werden.

Ausgaben von Systemen, die als sensibel oder betriebswichtig eingestufte Informationen enthalten, sollten 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 Werten

Maßnahme

Verfahren für die Handhabung von Werten sollten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.

Anleitung zur Umsetzung

Es sollten Verfahren eingeführt werden für die Handhabung, Verarbeitung, Speicherung und Kommunikation von Informationen entsprechend ihrer Klassifizierung (siehe 8.2.1).

Die folgenden Punkte sollten dabei berücksichtigt werden:

- a) Zugriffsbeschränkungen zur Unterstützung der Schutzanforderungen für jede Klassifizierungsstufe;
- b) Pflege eines formalen Verzeichnisses der befugten 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 berechtigten 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 Datenträgern

Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist, wird unterbunden.

8.3.1 Handhabung von Wechseldatenträgern

Maßnahme

Verfahren für die Handhabung von Wechseldatenträgern sollten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt werden.

Anleitung zur Umsetzung

Die folgenden Richtlinien für die Handhabung von Wechselmedien sollten beachtet werden:

- a) nicht mehr benötigte Inhalte auf wiederverwendbaren Datenträgern, welche vorgesehen sind, aus der Organisation entfernt zu werden, sollten so gelöscht werden, dass sie nicht wiederherstellbar sind;
- b) sofern notwendig und praktikabel ist, sollte für das Entfernen von Datenträgern aus der Organisation eine Genehmigungspflicht eingeführt werden und Aufzeichnungen über derartiges Entfernen aufbewahrt werden, um eine Prüfpfad aufrechtzuerhalten;
- c) sämtliche Datenträger 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 Daten auf Wechselmedien mittels Verschlüsselungsverfahren geschützt 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 Datenträger überwacht werden.

Verfahren und Berechtigungsebenen sollten dokumentiert werden.

8.3.2 Entsorgung von Datenträgern

Maßnahme

Nicht mehr benötigte Datenträger sollten sicher und unter Anwendung formaler Verfahren entsorgt werden.

Anleitung zur Umsetzung

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

- a) Datenträger, die vertrauliche Daten enthalten, sollten sicher gelagert und sicher entsorgt werden, z. B. durch Verbrennung oder Schreddern oder durch Löschung der Daten, falls der Datenträger von einer anderen Anwendung innerhalb der Organisation verwendet wird;
- 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 zu versuchen diejenigen Datenträger herauszusuchen, die tatsächlich sensible Daten enthalten;
- d) viele Organisationen bieten die Sammlung und Beseitigung von Datenträgern als Dienstleistung 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 Datenträgern mit sensiblen Daten sollte protokolliert werden, um einen Prüfpfad aufrechtzuerhalten.

Bei der Sammlung zur Entsorgung bestimmter Datenträger sollte darauf geachtet werden, auf den Kumulierungseffekt werden, dass eine große Menge einzeln nicht sensibler Information durch einen Kumulierungseffekt zusammengenommen einen Bestand sensibler Information darstellen kann.

Weitere Informationen

Beschädigte Datenträger, die sensible Daten enthalten, bedürfen möglicherweise einer Risikoeinschätzung, um zu bestimmen, ob diese Datenträger physisch zerstört, zur Reparatur versandt oder anderweitig ausgesondert werden sollten (siehe auch Abschnitt 11.2.7).

8.3.3 Transport von Datenträgern

Maßnahme

Datenträger, die Information enthalten, sollten während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden.

Anleitung zur Umsetzung

Die folgenden Leitfäden sollten berücksichtigt werden, um Datenträger mit Information während des Transportes zu schützen:

- a) es sollten zuverlässige Transport- bzw. Kurierdienstleister beauftragt werden;
- b) mit der Leitung sollte eine Liste befugter Kurierdienste vereinbart werden;
- c) es sollten Verfahren entwickelt werden, um die Identität der Kuriere sicher festzustellen;
- d) die Verpackung sollte ausreichend sein, um die Inhalte 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 elektromagnetischen Feldern betrifft, welche die Wiederherstellungsfähigkeit der Datenträger herabsetzen können;
- e) es sollten Protokolle geführt werden, aus denen der Inhalt der Datenträger, 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 Datenträger z. B. über einen Postdienstleister oder per Kurier versandt werden. Im Rahmen dieser Maßnahme gehören zu den Datenträgern auch Papierdokumente.

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

9 Zugangssteuerung^{N3)}

9.1 Geschäftsanforderungen an die Zugangsteuerung

Ziel: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt.

9.1.1 Zugangssteuerungsrichtlinie

Maßnahme

Eine Zugangssteuerungsrichtlinie sollte auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft werden.

N3) Nationale Fußnote: Der Zugang kann sowohl physisch als auch logisch erfolgen.

Anleitung zur Umsetzung

Zuständige für Werte sollten entsprechende Zugangssteuerungsregeln, Zugangsrechte und -beschränkungen für bestimmte Benutzerfunktionen in Bezug auf ihre Werte bestimmen, und zwar mit einer Detailliertheit und Strenge, welche die Informationssicherheitsrisiken widerspiegeln.

Zugangssteuerungen sind sowohl logischer als auch physischer Art (siehe Abschnitt 11) und beide Arten sind zusammen zu berücksichtigen. Benutzern und Dienstleistern gegenüber sollte eine klare Aussage hinsichtlich der geschäftlichen Anforderungen gemacht werden, die diese Zugangssteuerungen erfüllen sollen.

Die Richtlinie sollte die folgenden Punkte berücksichtigen:

- a) Sicherheitsanforderungen von Geschäftsanwendungen;
- b) Richtlinien zur Verteilung von Informationen und zur Genehmigung des Zugangs 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 Informationsklassifizierungsrichtlinien für Systeme und Netzwerke;
- d) Relevante Gesetzgebung und vertragliche Verpflichtungen hinsichtlich der Begrenzung des Zugangs auf Daten oder Dienstleistungen (siehe 18.1);
- e) Verwaltung von Zugangsrechten in einer verteilten und vernetzten Umgebung, welche alle verfügbaren Verbindungsarten berücksichtigt;
- f) Trennung von Zugangssteuerungsrollen, z. B. Zugangsbeantragung, Zugangsgenehmigung, Zugangsverwaltung;
- g) Anforderungen für die offizielle Genehmigung von Zugangsbeantragungen (siehe 9.2.1 und 9.2.2);
- 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 welche die Nutzung und Verwaltung von Benutzeridentitäten sowie geheimer Authentisierungsinformation betreffen;
- k) Rollen mit privilegiertem Zugriff (siehe 9.2.3).

Weitere Informationen

Bei der Festlegung der Zugangssteuerungsregeln sollte mit besonderer Sorgfalt vorgegangen werden, um die folgenden Punkte zu berücksichtigen:

- a) Festlegen von Regeln auf Grundlage der Prämisse, dass grundsätzlich alles verboten ist, was nicht ausdrücklich gestattet wird anstatt der schwächeren Regel das grundsätzlich alles erlaubt ist, sofern es nicht ausdrücklich verboten ist;
- b) Änderungen bei der Kennzeichnung von Informationen (siehe 8.2.2), die automatisch durch Einrichtungen zur Informationsverarbeitung und solche, die nach Ermessen eines Benutzers ausgelöst werden (siehe 8.2.2);

- c) Änderungen von Benutzerberechtigungen, die automatisch durch das Informationssystem und solche, die durch einen Administrator ausgelöst werden;
- d) Regeln, für deren Inkrafttreten eine Genehmigung erforderlich bzw. nicht erforderlich ist.

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

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

Zwei der häufigsten Prinzipien, die die Richtlinie zur Zugangssteuerung 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 Zugang auf diejenigen Netzwerke und Netzwerkdienste haben, zu deren Nutzung sie ausdrücklich befugt sind.

Anleitung zur Umsetzung

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

- a) die Netzwerke und Netzwerkdienste, zu denen Zugang gewährt wird;
- b) Genehmigungsverfahren zum Festlegen wem Zugang zu welchen Netzwerken und Netzwerkdiensten gewährt wird;
- c) Verwaltung der Steuerung und Verfahren zum Schutz des Zugangs zu Netzwerkverbindungen und Netzwerkdiensten;
- d) die verwendeten Mittel für den Zugang zu Netzwerken und Netzwerkdiensten (z. B. Nutzung von VPN oder WLAN);
- e) Anforderungen bezüglich der Benutzerauthentifizierung für den Zugang zu verschiedenen Netzwerkdiensten;
- f) Überwachung der Nutzung von Netzwerkdiensten.

Die Richtlinie zur Nutzung von Netzwerkdiensten sollte konsistent mit der Zugangssteuerungsrichtlinie der Organisation sein (siehe 9.1.1).

Weitere Informationen

Unbefugte und unsichere Verbindungen zu Netzwerkdiensten können Auswirkungen auf die gesamte Organisation haben. Diese Maßnahme ist insbesondere wichtig für Netzwerkverbindungen zu sensiblen oder