DEUTSCHE NORM **Entwurf** **Februar 2014**

DIN ISO/IEC 27002

DIN

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

Preisgruppe 31
www.din.de
www.beuth.de

2073178

Inhalt

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-Mangamentsysteme — Überblick und Terminolgie*

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 angegeben 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 heben 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 ernennt, 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 Aufgabetrennung 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 festlegt 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 Mitarbeiten 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 Managements

Maßnahme

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 zusammengenommen 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:

a) Die Netzwerke und Netzwerkdienste, zu denen Zugang gewährt wird;

b) Genehmigungsverfahren zur Bestimmung der Personen, denen der Zugang zu Netzwerken und Netzwerkdiensten gewährt wird;

c) Verwaltung der Kontrollen und Verfahren zum Schutz des Zugang 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 der Zugangskontrollleitlinie der Organisation entsprechen (siehe 9.1.1).

Weitere Informationen

Nicht autorisierte und unsichere Verbindungen zu Netzwerkdiensten können Auswirkungen auf die gesamte Organisation haben. Diese Maßnahme ist insbesondere wichtig für Netzwerkverbindungen zu sensiblen oder betriebswichtigen Geschäftsanwendungen oder zu Benutzern an Hochrisikostandorten wie z. B. öffentlichen oder externen Bereichen, die sich außerhalb des Einflussbereichs des Informationssicherheits- und -kontrollsystems der Organisation befinden.

9.2 Benutzerverwaltung

Zielsetzung: Sicherstellung des Zugangs ausschließlich für autorisierte Benutzer und Verhinderung von nicht autorisiertem Zugang zu Systemen und Diensten.

9.2.1 An- und Abmeldung von Benutzern

Maßnahme

Ein formeller Anmeldungs- und Abmeldungsprozess für Benutzer sollte implementiert werden, um die Zuweisung von Benutzerberechtigungen zu ermöglichen.

Umsetzungshinweise

Der Prozess zur Verwaltung der Benutzerkennungen sollte folgende Punkte umfassen:

a) Verwendung eindeutiger Benutzerkennungen, damit Benutzer mit ihren Handlungen in Verbindung gebracht und verantwortlich gemacht werden können. Die Verwendung gemeinsam genutzter Kennungen sollte nur gestattet werden, wenn dies aus geschäftlichen oder betrieblichen Gründen erforderlich ist und sollte genehmigt und dokumentiert werden;

b) sofortige Deaktivierung bzw. Löschung der Kennungen von Benutzern, die die Organisation verlassen haben (siehe 9.2.5);

c) regelmäßige Feststellung und Löschung bzw. Deaktivierung ehemals genutzter Benutzerkennungen;

d) Sicherstellung, dass ehemals genutzte Kennungen nicht an andere Benutzer vergeben werden.

Weitere Informationen

Die Gewährung bzw. der Entzug des Zugangs zu Informationen oder Einrichtungen zur Informationsverarbeitung erfolgt normalerweise im Rahmen eines zweistufigen Verfahrens:

a) Zuweisung und Aktivierung bzw. Entziehung einer Benutzerkennung (diese Maßnahme);

b) Gewährung bzw. Entziehung der Zugangsrechte zu dieser Benutzerkennung (siehe 9.2.2).

9.2.2 Zugangsbereitstellung für Benutzer

Maßnahme

Ein formeller Zugangsbereitstellungsprozess für Benutzer sollte implementiert werden, um Zugangsrechte für alle Benutzertypen zu allen Systemen und Diensten zuzuweisen bzw. zu entziehen.

Umsetzungshinweise

Der Bereitstellungsprozess für die Zuweisung bzw. Entziehung der dem Benutzer unter seiner Kennung gewährten Zugangsrechte sollte folgende Punkte umfassen:

a) Erhalt der Berechtigung vom Eigentümer des Informationssystems oder Dienste zur Nutzung des Informationssystems oder Dienstes (siehe Maßnahme 8.1.2), wobei eine separate Genehmigung von Zugangsrechten durch das Management ebenfalls angemessen sein kann;

b) Verifizierung, dass die gewährte Berechtigungsstufe den Zugangsrichtlinien angemessen ist (siehe 9.1) und den anderen Anforderungen wie der Aufgabentrennung (siehe 6.1.5) entspricht;

c) Sicherstellung, dass die Zugangsrechte nicht aktiviert werden (z. B. durch die Dienstleister), bevor die Genehmigungsverfahren abgeschlossen sind;

d) Pflege eines zentralen Verzeichnisses der einem Benutzer unter seiner Kennung gewährten Rechte für den Zugang zu Informationssystemen und Diensten;

e) Anpassung der Zugangsrechte der Benutzer, deren Funktionen oder Tätigkeit sich geändert haben und unverzügliche Entziehung oder Blockierung der Berechtigungen von Benutzern, die die Organisation verlassen haben;

f) Regelmäßige Überprüfung der Zugangsrechte zusammen mit den Eigentümern der Informationssysteme und Dienste (siehe 9.2.4).

Weitere Informationen

Es sollte überlegt werden, Benutzerzugangsfunktionen auf Grundlage von geschäftlichen Anforderungen zu definieren, in denen eine Anzahl von Zugangsrechten zu typischen Benutzerzugangsprofilen zusammengefasst werden. Zugangsbeantragungen und -überprüfungen (siehe 9.2.4) lassen sich auf der Ebene derartiger Funktionen einfacher verwalten als auf der Ebene von Einzelberechtigungen.

Es sollte überlegt werden, Klauseln in Anstellungs- und Dienstleistungsverträge aufzunehmen, in denen Sanktionen für den Fall spezifiziert werden, dass ein nicht autorisierter Zugriff durch einen Mitarbeiter oder Auftragnehmer versucht wird (siehe 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Verwaltung von Sonderzugangsrechten

Maßnahme

Die Zuteilung und Nutzung von Sonderzugangsrechten sollte eingeschränkt und kontrolliert werden.

Umsetzungshinweise

Die Zuteilung von Sonderzugangsrechten sollte durch einen offiziellen Genehmigungsprozess entsprechend der jeweiligen Zugangskontrollleitlinie (siehe Maßnahme 9.1.1) kontrolliert werden. Die folgenden Schritte sollten dabei berücksichtigt werden:

a) Die Sonderzugangsrechte, die mit den einzelnen Systemen oder Prozessen verbunden sind, z. B. Betriebssystem, Datenbankverwaltungssystem und jede Anwendung sowie die Benutzer, denen sie zugewiesen werden, müssen festgestellt werden;

b) Sonderzugangsrechte sollten Benutzern nur im Bedarfsfall und ereignisbezogen entsprechend der Zugangskontrollleitlinie (siehe 9.1.1) erteilt werden, d. h. auf Grundlage der Mindestanforderungen für ihre Funktionsbereiche;

c) Es sollten ein Genehmigungsprozess und eine aktuelle Aufstellung aller gewährten Sonderrechte existieren. Sonderzugangsrechte sollten nicht vor Abschluss des Genehmigungsprozesses gewährt werden;

d) Es sollten Anforderungen bezüglich des Auslaufens von Sonderzugangsrechten festgelegt werden;

e) Sonderzugangsrechte sollten einer anderen als der Benutzerkennung zugewiesen werden, die für die normalen Geschäftsaktivitäten verwendet wird. Normale Geschäftsaktivitäten sollten nicht mit Konten ausgeführt werden, die über Sonderzugangsrechte verfügen;

f) Die Kompetenzen von Benutzern mit Sonderzugangsrechten sollten regelmäßig überprüft werden, um sicherzustellen, dass sie deren Aufgabenprofil entsprechen;

g) Es sollten spezifische Verfahren eingerichtet und angewendet werden, mit denen eine nicht autorisierte Nutzung von Benutzerkennungen mit allgemeinen Administratorrechten im Rahmen der Konfigurationsmöglichkeiten des Systems verhindert wird;

h) In Bezug auf Benutzerkennungen mit allgemeinen Administratorrechten sollte die Vertraulichkeit der geheimen Authentifizierungsdaten bei einer gemeinsamen Nutzung gewahrt werden (z. B. häufige Änderung der Kennwörter sowie nach Ausscheiden oder Versetzung eines Benutzers mit Sonderzugangsrechten deren möglichst zeitnahe Mitteilung an Benutzer mit Sonderzugangsrechten mittels geeigneter Mechanismen).

Weitere Informationen

Eine unangemessene Nutzung von Systemadministratorrechten (d. h. einer Funktion oder Einrichtung eines Informationssystems, mit deren Hilfe der Benutzer die System- oder Anwendungskontrollen außer Kraft setzen kann) kann maßgeblich zu Systemfehlern oder einer Beeinträchtigung der Systemsicherheit beitragen.

9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern

Maßnahme

Die Zuweisung von geheimen Authentifizierungsdaten sollte über einen formellen Verwaltungsprozess kontrolliert werden.

Umsetzungshinweise

Der Prozess sollte den folgenden Anforderungen genügen:

a) Die Benutzer sollten dazu verpflichtet werden, eine Erklärung zu unterzeichnen, dass sie die persönlichen, geheimen Authentifizierungsdaten vertraulich behandeln und als Gruppendaten (also gemeinsam) genutzte geheime Authentifizierungsdaten ausschließlich unter den Mitglieder der Gruppe austauschen. Diese unterzeichnete Erklärung kann als Bestandteil der Beschäftigungsbedingungen (siehe 7.1.2) aufgenommen werden;

b) Wenn es erforderlich ist, Benutzern eigene geheime Authentifizierungsdaten zu gewähren, sollten ihnen zunächst temporär gültige geheime Authentifizierungsdaten zugestellt werden, die sich bei der ersten Verwendung ändern müssen;

c) Es sollten Verfahren eingerichtet werden, mit denen die Identität eines Benutzers vor der Zustellung neuer, die bisherigen ersetzender oder temporär gültiger geheimer Authentifizierungsdaten überprüft werden kann;

d) Temporär gültige geheime Authentifizierungsdaten sollten dem Benutzer auf sicherem Wege übermittelt werden. Die Nutzung externer Parteien oder unverschlüsselter (Klartext-)E-Mail-Nachrichten sollte vermieden werden;

e) Temporär gültige Authentifizierungsdaten sollten nur einmalig und an eine bestimmte Person gebunden verwendet werden und nicht zu erschließen sein;

f) Die Benutzer sollten den Erhalt der sicheren Authentifizierungsdaten quittieren;

g) Nach der Installation von Systemen und Software sollten die vorgegebenen Authentifizierungsdaten des Anbieters geändert werden.

Weitere Informationen

Kennwörter sind eine allgemein gebräuchliche Art von Authentifizierungsdaten und ein übliches Mittel zur Verifizierung der Identität eines Benutzers. Andere Arten von geheimen Authentifizierungsdaten sind kryptografische Schlüssel und andere auf Hardware-Token (z.B. Smartcards) gespeicherte Daten, die Authentifizierungscodes erzeugen.

9.2.5 Überprüfung von Benutzerberechtigungen

Maßnahme

Werteeigentümer sollten die Benutzerberechtigungen in regelmäßigen Abständen prüfen.

Umsetzungshinweise

Bei der Überprüfung der Benutzerberechtigungen sollten die folgenden Punkte beachtet werden:

a) Die Benutzerberechtigungen sollten in regelmäßigen Abständen und nach jeder Änderung, z. B. durch Beförderung, Herabstufung oder Beendigung des Arbeitsverhältnisses (siehe 7), überprüft werden;

b) Benutzerberechtigungen sollten bei Wechseln innerhalb der Organisation von einem Funktionsbereich in einen anderen überprüft und neu zugewiesen werden;

c) Genehmigungen von Sonderzugangsrechten sollten in kürzeren Abständen überprüft werden;

d) Die Gewährung von Sonderzugangsrechten sollte in regelmäßigen Abständen überprüft werden, um sicherzustellen, dass keine nicht autorisierten Befugnisse erworben wurden;

e) Änderungen bei Konten mit Sonderzugangsrechten sollten zur regelmäßigen Überprüfung protokolliert werden.

Weitere Informationen

Diese Maßnahme wirkt möglichen Schwachpunkten bei der Ausführung der Maßnahmen in 9.2.1, 9.2.2 und 9.2.6 entgegen.

9.2.6 Entziehung oder Anpassung von Zugangsrechten

Maßnahme

Die Zugangsrechte aller Mitarbeiter und externen Benutzer zu Informationen und informationsverarbeitenden Einrichtungen sollten nach Beendigung des Beschäftigungsverhältnisses, des Vertrags bzw. der Vereinbarung entzogen bzw. bei dessen Änderung entsprechend angepasst werden.

Umsetzungshinweise

Bei Beendigung sollten die Zugangsrechte einer Person in Bezug auf Informationen und Werte im Zusammenhang mit Einrichtungen zur Informationsverarbeitung und Dienste entzogen oder ausgesetzt werden. Damit kann ermittelt werden, ob es erforderlich ist, Zugangsrechte zu entziehen. Änderungen im Beschäftigungsverhältnis sollten sich in der Entziehung sämtlicher Zugangsrechte widerspiegeln, die für die neue Tätigkeit nicht genehmigt wurden. Zu den zu entziehenden Zugangsrechten gehören physische ebenso wie logische Zugangsrechte. Die Entziehung oder Anpassung kann mittels Entfernung, Sperrung oder Ersetzung von Schlüsseln, Ausweiskarten, Einrichtungen zur Informationsverarbeitung oder Abonnements erfolgen. Dokumente, in denen die Zugangsrechte von Mitarbeitern und Auftragnehmern festgehalten sind, sollten bei Entziehung oder Anpassung von Zugangsrechten entsprechend aktualisiert werden. Wenn ein scheidender Mitarbeiter oder Auftragnehmer über bekannte Kennwörter für noch aktive Benutzerkennungen verfügt, sollten diese bei Beendigung oder Änderung des Beschäftigungs- bzw. Vertragsverhältnisses geändert werden.

Zugangsrechte in Bezug auf Informationen und Werte im Zusammenhang mit Einrichtungen zur Informationsverarbeitung sollten vor Ende bzw. bei Änderung des Beschäftigungsverhältnisses entweder eingeschränkt oder entzogen werden, wofür die Beurteilung unter anderem der folgenden Risikofaktoren ausschlaggebend ist:

a) Frage, ob die Beendigung oder Änderung vom Mitarbeiter, der externen Partei oder vom Management ausgeht, sowie die Gründe für die Beendigung;

b) die aktuellen Zuständigkeiten des Mitarbeiters, der externen Partei bzw. eines anderen Benutzers;

c) Einstufung der derzeit zugänglichen Werte.

Weitere Informationen

Unter bestimmten Umständen kann es vorkommen, dass Zugangsrechte nicht nur an den scheidenden Mitarbeiter oder externen Benutzer, sondern an mehrere Personen vergeben wurden (z. B. Gruppenkennungen). In diesen Fällen sollten scheidende Mitarbeiter aus allen Gruppenzugangslisten entfernt und Maßnahmen getroffen werden, alle anderen betroffenen Mitarbeiter und externen Benutzer darauf hinzuweisen, dass sie diese Daten nicht mehr mit der scheidenden Person teilen dürfen.

Bei einer vom Management ausgehenden Beendigung des Arbeits- oder Vertragsverhältnisses kann es dazu kommen, dass darüber verärgerte Mitarbeiter oder externe Benutzer vorsätzlich Daten verfälschen oder Einrichtungen zur Informationsverarbeitung sabotieren. Personen, die selbst kündigen oder denen gekündigt wird, können der Versuchung erliegen, Daten zur späteren Verwendung zu sammeln.

9.3 Benutzerverantwortung

Zielsetzung: Übertragung der Verantwortung für den Schutz der Authentifizierungsdaten auf die Benutzer

9.3.1 Verwendung geheimer Authentifizierungsdaten von Benutzern

Maßnahme

Von den Benutzern sollte verlangt werden, die Praktiken der Organisation zur Verwendung von geheimen Authentifizierungsdaten zu befolgen.

Umsetzungshinweise

Alle Benutzer sollten angewiesen werden, die folgenden Grundsätze zu beachten:

a) Geheime Authentifizierungsdaten müssen vertraulich behandelt werden, um sicherzustellen, dass sie nicht in die Hände Dritter einschließlich der Behörden geraten;

b) Geheime Authentifizierungsdaten sollten nicht notiert oder gespeichert werden (z. B. auf Papier, in einer Datei oder auf einem Mobilgerät), es sei denn, dass dieses Medium sicher aufbewahrt werden kann und diese Aufbewahrungsmethode genehmigt wurde (z. B. Kennwortverwaltung) ;

c) Bei jedweden Anzeichen einer möglichen Kompromittierung der geheimen Authentifizierungsdaten sind diese unverzüglich zu ändern;

d) Falls Kennwörter zur sicheren Authentifizierung verwendet werden, sind starke Kennwörter ausreichender Mindestlänge zu wählen, die

   1) einfach zu merken sind;

   2) auf keinen Sachverhalten basieren, das eine andere Person unter Zuhilfenahme personenbezogener Daten wie z. B. Namen, Telefonnummern, Geburtstage usw. einfach erraten oder erschließen kann;

   3) nicht anfällig für Wörterbuchangriffe sind (d. h. nicht aus Wörtern bestehen, die im Wörterbuch stehen);

   4) keine Folge identischer, numerischer oder alphanumerischer Zeichen enthalten;

   5) bei der ersten Anmeldung geändert werden, wenn es sich um temporäre Kennwörter handelt.

e) Die eigenen, geheimen Authentifizierungsdaten dürfen keiner anderen Person mitgeteilt werden;

f) Wenn Kennwörter zur sicheren Authentifizierung im Rahmen von automatisierten Anmeldeverfahren verwendet und gespeichert werden, ist für einen ordnungsnachen Kennwortschutz zu sorgen;

g) Für geschäftliche und nicht geschäftliche Zwecke dürfen nicht dieselben geheimen Authentifizierungsdaten verwendet werden.

Weitere Informationen

Durch die Bereitstellung von Single Sign On (SSO) oder anderer Verwaltungstools für geheime Authentifizierungsdaten verringert sich die Menge geheimer Authentifizierungsdaten, die die Benutzer schützen müssen, so dass auf diese Weise die Effektivität dieser Maßnahme gesteigert werden kann. Allerdings kann sich bei Verwendung dieser Tools die Offenlegung geheimer Authentifizierungsdaten auch schwerwiegender auswirken.

9.4 Kontrolle des Zugangs zu Systemen und Anwendungen

Zielsetzung: Verhinderung des nicht autorisierten Zugangs zu Systemen und Anwendungen.

9.4.1 Beschränkung des Zugangs zu Informationen

Maßnahme

Der Zugang zu Funktionen von Informations- und Anwendungssystemen sollte entsprechend der Zugangskontrollleitlinie beschränkt werden.

Umsetzungshinweise

Zugangsbeschränkungen sollten aufgrund der Anforderungen einzelner Geschäftsanwendungen und entsprechend der festgelegten Zugangskontrollleitlinie erfolgen.

Die folgenden Punkte sollten zur Unterstützung der Zugangsbeschränkungsanforderungen berücksichtigt werden:

a) Bereitstellung von Menüs zur Kontrolle des Zugangs zu Funktionen des Anwendungssystems;

b) Kontrolle bezüglich der Daten, zu denen ein Benutzer Zugang hat;

c) Kontrolle der Zugangsrechte von Benutzern (z. B. lesen, schreiben, löschen, ausführen);

d) Kontrolle der Zugangsrechte zu anderen Anwendungen;

e) Beschränkung der in den Ausgabedaten enthaltenen Informationen;

f) Bereitstellung physischer oder logischer Zugangskontrollen zur Isolierung sensibler Anwendungen, Anwendungsdaten oder Systeme.

9.4.2 Sichere Anmeldeverfahren

Maßnahme

Der Zugang zu Systemen und Anwendungen sollte über ein sicheres Anmeldeverfahren kontrolliert werden, wenn dies nach der Zugangskontrollleitlinie erforderlich ist.

Umsetzungshinweise

Es sollte ein geeignetes Authentifizierungsverfahren zur Bestätigung der Identität des Benutzers gewählt werden.

Sofern eine starke Authentifizierung und Identitätsverifizierung erforderlich ist, sollten Authentifizierungsalternativen zu Kennwörtern wie kryptografische Verfahren, Smartcards, Token oder biometrische Technologien verwendet werden.

Das Verfahren zur Anmeldung in einem System oder einer Anwendung sollte so gestaltet sein, dass die Gefahr eines nicht autorisierten Zugangs möglichst gering ist. Das Anmeldeverfahren sollte daher so wenig Informationen wie möglich über das System oder die Anwendung preisgeben, um einem nicht autorisierten Benutzer keine unnötige Hilfestellung zu geben. Ein gutes Anmeldeverfahren sollte sich durch folgende Punkte auszeichnen:

a) Es werden keine System- oder Anwendungsinformationen angezeigt, bis der Anmeldeprozess erfolgreich abgeschlossen wurde;

b) Es wird eine allgemeine Warnmeldung angezeigt, dass nur autorisierte Benutzer Zugang zum Computer haben sollten;

c) Während des Anmeldeverfahrens werden keine Hilfetexte angezeigt, die sich Unbefugte zunutze machen könnten;

d) Die Anmeldedaten werden erst nach Eingabe aller Daten geprüft. Bei Auftreten eines Fehlers sollte das System nicht anzeigen, welcher Teil der eingegebenen Daten richtig oder nicht richtig war;

e) Es besteht ein Schutz vor Brute-Force-Anmeldeversuchen;

f) Erfolglose und erfolgreiche Anmeldeversuche werden protokolliert;

g) Bei Erkennung einer möglicherweise versuchten oder erfolgreichen Umgehung der Anmeldekontrolle wird ein Sicherheitsereignis ausgelöst;

h) Nach erfolgreicher Anmeldung werden die folgenden Daten angezeigt;

   1) Datum und Uhrzeit der letzten erfolgreichen Anmeldung;

   2) Einzelheiten zu erfolglosen Anmeldeversuchen seit der letzten erfolgreichen Anmeldung.

i) Das eingegebene Kennwort wird nicht angezeigt;

j) Kennwörter werden nicht im Klartext über das Netzwerk übertragen;

k) Inaktive Sitzungen werden nach einer vorgegebenen Zeitspanne beendet, insbesondere an Hochrisiko-Standorten wie in öffentlichen oder externen Bereichen, die nicht dem Sicherheitsmanagement der Organisation unterstehen, oder auf Mobilgeräten;

l) Verbindungszeiten werden beschränkt, um zusätzliche Sicherheit bei Hochrisikoanwendungen zu bieten und möglichst wenig Gelegenheit für nicht autorisierte Zugangsversuche zu bieten.

Weitere Informationen

Kennwörter sind ein gebräuchliches Verfahren zur Identifizierung und Authentifizierung mittels eines Geheimnisses, das nur der Benutzer kennt. Gleiches kann mit kryptografischen Verfahren und Authentifizierungsprotokollen erreicht werden. Die Stärke einer Benutzerauthentifizierung sollte der Klassifizierung der Daten angemessen sein, auf die zugegriffen werden soll.

Wenn Kennwörter während der Anmeldung im Klartext über ein Netzwerk übertragen werden, können sie von einem sogenannten Sniffer-Programm ausgespäht werden.

9.4.3 Kennwortmanagementsystem

Maßnahme

Kennwortmanagementsysteme sollten interaktiv sein und starke Kennwörter erfordern.

Umsetzungshinweise

Ein Kennwortmanagementsystem sollte sich durch folgende Punkte auszeichnen:

a) Es sollte die Verwendung individueller Benutzerkennungen und Kennwörter erfordern, um die Verantwortlichkeit des einzelnen Benutzers sicherzustellen;

b) Es sollte den Benutzern die Möglichkeit bieten, eigene Kennwörter zu wählen und diese zu ändern sowie ein Bestätigungsverfahren beinhalten, das Eingabefehler abfängt;

c) Es sollte sicherstellen, dass starke Kennwörter gewählt werden;

d) Es sollte die Benutzer auffordern, ihr Kennwort bei der ersten Anmeldung zu ändern;

e) Es sollte zu Kennwortänderungen in regelmäßigen Abständen sowie bei Bedarf auffordern;

f) Es sollte eine Liste zuvor verwendeter Kennwörter pflegen, um eine erneute Verwendung zu verhindern;

g) Es sollte Kennwörter bei der Eingabe nicht auf dem Bildschirm anzeigen;

h) Es sollte Kennwörter getrennt von den Anwendungssystemdaten speichern;

i) Es sollte Kennwörter verschlüsselt speichern und übertragen.

Weitere Informationen

Bei einigen Anwendungen sind Kennwörter erforderlich, die von unabhängiger Seite vergeben werden. In derartigen Fällen finden die Punkte b), d) und e) keine Anwendung. In den meisten Fällen werden die Kennwörter jedoch von den Benutzern gewählt und verwaltet.

9.4.4 Verwendung von Systemwerkzeugen

Maßnahme

Die Verwendung von Dienstprogrammen, mit denen sich u. U. System- und Anwendungskontrollen umgehen lassen, sollte beschränkt und streng kontrolliert werden.

Umsetzungshinweise

Die folgenden Leitlinien für die Verwendung von Dienstprogrammen, mit denen sich u. U. System- und Anwendungskontrollen umgehen lassen, sollten beachtet werden:

a) Verwendung von Identifizierungs-, Authentifizierungs- und Genehmigungsverfahren für Dienstprogramme;

b) Trennung der Dienstprogramme von der Anwendungssoftware;

c) Beschränkung der Verwendung von Dienstprogrammen auf eine möglichst geringe Zahl vertrauenswürdiger, autorisierter Benutzer (siehe 9.2.2);

d) Genehmigung zur Ad-hoc-Verwendung von Dienstprogrammen;

e) Beschränkung der Verfügbarkeit von Dienstprogrammen, z. B. auf die Dauer einer autorisierten Änderung;

f) grundsätzliche Protokollierung der Verwendung von Dienstprogrammen;

g) Festlegung und Dokumentation von Berechtigungsstufen für Dienstprogramme;

h) Entfernung bzw. Deaktivierung aller nicht notwendiger Dienstprogramme;

i) Sperrung von Dienstprogrammen für Benutzer, die Zugang zu Anwendungen auf Systemen haben, bei denen eine Aufgabentrennung erforderlich ist.

Weitere Informationen

Die meisten Computerinstallationen verfügen über mindestens ein Dienstprogramm, mit dem sich System- und Anwendungskontrollen umgehen lassen.

9.4.5 Kontrolle des Zugriffs auf Software-Quellcode

Maßnahme

Der Zugriff auf den Software-Quellcode sollte beschränkt werden.

Umsetzungshinweise

Der Zugriff auf den Software-Quellcode und zugehörige Objekte (wie Entwürfe, Spezifikationen, Verifizierungs- und Validierungspläne) sollte streng kontrolliert werden, um die Hinzufügung nicht autorisierter Funktionen zu verhindern und unbeabsichtigte Änderungen zu vermeiden sowie um die Vertraulichkeit des wertvollen geistigen Eigentums zu gewährleisten. Bezüglich des Software-Quellcodes kann dies durch kontrollierte zentrale Speicherung, vorzugsweise in Software-Quellcode-Bibliotheken, erreicht werden. In diesem Fall sollten die folgenden Leitlinien beachtet werden, um den Zugang zu diesen Software-Quellcode-Bibliotheken zu kontrollieren und die Gefahr einer Verfälschung der Computerprogramme zu verringern:

a) Die Software-Quellcode-Bibliotheken sollten möglichst nicht in Betriebssystemen vorgehalten werden;

b) Der Software-Quellcode und die Software-Quellcode-Bibliotheken sollten nach festgelegten Verfahren verwaltet werden;

c) Die Support-Mitarbeiter sollten über keinen uneingeschränkten Zugriff auf die Software-Quellcode-Bibliotheken verfügen;

d) Die Aktualisierung der Software-Quellcode-Bibliotheken und der zugehörigen Objekte sowie die Herausgabe von Software-Quellcode an Programmierer sollte erst nach Erhalt der entsprechenden Autorisierung erfolgen;

e) Die Software-Listings sollten in einer gesicherten Umgebung aufbewahrt werden;

f) Sämtliche Zugriffe auf Software-Quellcode-Bibliotheken sollten in einem Audit-Protokoll festgehalten werden;

g) Die Pflege und Kopie der Software-Quellcode-Bibliotheken sollte strengen Änderungskontrollverfahren (siehe 14.2.2) unterliegen.

Wenn eine Veröffentlichung des Software-Quellcodes vorgesehen ist, sollten zusätzliche Sicherheitsmaßnahmen in Betracht gezogen werden, um die Integrität des Codes (z. B. mittels einer digitalen Signatur) sicherzustellen.

10 Kryptographie

10.1 Kryptographische Maßnahmen

Zielsetzung: Sicherstellung der ordnungsnachen und wirksamen Verwendung von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und/oder Integrität von Informationen.

10.1.1 Leitlinie zur Nutzung von kryptographischen Maßnahmen

Maßnahme

Eine Leitlinie zur Verwendung von kryptographischen Maßnahmen für den Schutz von Informationen sollte entwickelt und implementiert werden.

Umsetzungshinweise

Bei der Entwicklung einer Kryptographie-Leitlinie sollten die folgenden Punkte berücksichtigt werden:

a) der Managementansatz bezüglich der Verwendung kryptographischer Maßnahmen innerhalb der Organisation, einschließlich der allgemeinen Prinzipien, nach denen geschäftliche Daten geschützt werden sollten;

b) auf Grundlage einer Risikoeinschätzung sollte die erforderliche Schutzstufe unter Berücksichtigung der Art, Stärke und Qualität des erforderlichen Verschlüsselungsalgorithmus bestimmt werden;

c) die Verwendung von Verschlüsselungstechnologien zum Schutz von Daten, die auf mobilen oder Wechselmedienträgern transportiert oder über Telekommunikationsleitungen übertragen werden;

d) der Ansatz zur Verwaltung kryptographischer Schlüssel, einschließlich Methoden zur Handhabung des Schutzes kryptographischer Schlüssel und der Wiederherstellung verschlüsselter Daten im Falle verlorener, kompromittierter oder beschädigter Schlüssel;

e) Aufgaben und Zuständigkeiten, z. B. bezüglich der Verantwortung für;

   1) die Umsetzung der Leitlinie;

   2) die Verwaltung der Schlüssel, einschließlich deren Erzeugung (siehe 10.1.2);

f) die zur wirksamen Umsetzung innerhalb der gesamten Organisation zu befolgenden Normen (die jeweiligen Lösungen für die verschiedenen Geschäftsabläufe);

g) die Auswirkung der Verwendung verschlüsselter Daten auf Maßnahmen, die auf der Überprüfung von Inhalten basieren (z. B. Malware-Erkennung).

Bei der Umsetzung der Kryptographie-Leitlinie der Organisation sollten die Vorschriften und nationalen Beschränkungen beachtet werden, die möglicherweise hinsichtlich der Verwendung von Verschlüsselungsverfahren in verschiedenen Teilen der Welt sowie in Bezug auf die grenzüberschreitende Übertragung verschlüsselter Daten gelten (siehe 18.1.5).

Kryptographische Maßnahmen können dazu verwendet werden, verschiedene Informationssicherheitsziele zu erreichen, z. B.:

a) Vertraulichkeit: Verwendung von Verschlüsselung zum Schutz sensibler oder betriebswichtiger, gespeicherter oder übertragener Daten;

b) Integrität/Authentizität: Verwendung digitaler Signaturen oder Authentifizierungscodes für Nachrichten zur Bestätigung der Authentizität bzw. Integrität gespeicherter oder übertragener sensibler oder betriebswichtiger Daten;

c) Unabstreitbarkeit: Verwendung von Verschlüsselungsverfahren zum Nachweis des Eintritts bzw. Nichteintritts eines Ereignisses oder einer Handlung;

d) Authentifizierung: Verwendung von Verschlüsselungsverfahren zur Authentifizierung von Benutzern und anderen Systementitäten, die Zugang zu oder Transaktionen mit Systembenutzern, -entitäten und -ressourcen beantragen.

Weitere Informationen

Die Entscheidung darüber, ob der Einsatz einer Verschlüsselungslösung angemessen ist, sollte als Teil eines allgemeineren Verfahrens zur Risikoeinschätzung und Auswahl von Sicherheitsmaßnahmen betrachtet werden. Diese Einschätzung kann anschließend zur Bestimmung der Angemessenheit eines Einsatzes kryptographischer Maßnahmen verwendet werden sowie für die Entscheidung über die Art der anzuwendenden Maßnahmen, den damit verfolgten Zweck und die dafür infrage kommenden Geschäftsabläufe.

Eine Leitlinie für den Einsatz kryptographischer Maßnahmen ist notwendig, um die Vorteile des Einsatzes von Verschlüsselungsverfahren voll auszuschöpfen, die damit verbundenen Risiken möglichst gering zu halten und eine unangemessene oder unsachgemäße Verwendung zu vermeiden.

Bei der Auswahl angemessener kryptographischer Maßnahmen sollten Fachleute herangezogen werden, um die Einhaltung der Ziele der Leitlinie zur Informationssicherheit zu gewährleisten.

10.1.2 Verwaltung kryptographischer Schlüssel

Maßnahme

Eine Leitlinie zur Verwendung, zum Schutz und zur Gültigkeitsdauer von kryptographischen Schlüsseln sollte entwickelt und über deren gesamten Nutzungsdauer hinweg umgesetzt werden.

Umsetzungshinweise

Die Leitlinie sollte Anforderungen zur Verwaltung kryptographischer Schlüssel über deren gesamte Nutzungsdauer hinweg beinhalten (Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung und Löschung).

Verschlüsselungsalgorithmen, Schlüssellängen und Verwendungsweisen sollten nach dem Grundsatz der „Best Practice“ ausgewählt werden. Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung und Löschung kryptographischer Schlüssel.

Alle kryptographischen Schlüssel sollten gegen Veränderung und Verlust geschützt sein. Zusätzlich sollten geheime und private Schlüssel gegen unbefugte Benutzung und Offenlegung geschützt werden. Einrichtungen zur Erzeugung, Speicherung und Archivierung von Schlüsseln sollten physisch geschützt sein.

Ein Schlüsselverwaltungssystem sollte auf einer Reihe anerkannter Normen, Verfahren und sicherer Methoden basieren:

a) zur Erzeugung von Schlüsseln für verschiedene Verschlüsselungssysteme und Anwendungen;

b) zur Ausstellung und zum Erhalt von Public-Key-Zertifikaten;

c) zur Verteilung von Schlüsseln an die entsprechenden Entitäten, einschließlich der Information, wie diese bei Erhalt zu aktivieren sind;

d) zur Speicherung von Schlüsseln, einschließlich der Information, wie autorisierte Benutzer Zugang zu diesen erhalten;

e) zur Änderung oder Aktualisierung von Schlüsseln, einschließlich der Regeln, die den richtigen Zeitpunkt sowie die Art und Weise der Änderung eines Schlüssels bestimmen;

f) zum Umgang mit kompromittierten Schlüsseln;

g) zum Widerruf von Schlüsseln, einschließlich der Art und Weise, wie Schlüssel zurückgezogen oder deaktiviert werden, z. B. wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten die Schlüssel auch archiviert werden);

h) zur Wiederherstellung verlorener oder verfälschter Schlüssel;

i) zur Sicherung oder Archivierung von Schlüsseln;

j) zur Löschung von Schlüsseln;

k) zur Protokollierung und Prüfung die Schlüsselverwaltung betreffender Aktivitäten.

Um die Wahrscheinlichkeit einer unsachnachen Verwendung zu verringern, sollten für die Aktivierung und Deaktivierung von Schlüsseln Festlegungen getroffen werden, so dass die Schlüssel nur über einen in der entsprechenden Leitlinie zur Schlüsselverwaltung vorgegebenen Zeitraum verwendet werden können.

Zusätzlich sollte zur sicheren Verwaltung der geheimen und privaten Schlüssel auch die Authentizität der öffentlichen Schlüssel berücksichtigt werden. Dieser Authentifizierungsprozess kann mit Hilfe von Public-Key-Zertifikaten erfolgen, die meist von einer Zertifizierungsstelle ausgestellt werden, bei der es sich um eine anerkannte Organisation handeln sollte, die über geeignete Kontrollen und Verfahren verfügt, um die erforderliche Vertrauenswürdigkeit sicherzustellen.

Die Service Level Agreements bzw. Verträge mit externen Anbietern von Verschlüsselungsdiensten, z. B. einer Zertifizierungsstelle, sollten Themen wie Haftung, Zuverlässigkeit der Dienste und Antwortzeiten für die Bereitstellung der Dienste (siehe 15.2) einschließen.

Weitere Informationen

Die Verwaltung der kryptographischen Schlüssel ist für die effektive Nutzung von Verschlüsselungsverfahren entscheidend. ISO/IEC 11770 enthält weitere Informationen zur Schlüsselverwaltung.

Verschlüsselungsverfahren können auch zum Schutz kryptographischer Schlüssel genutzt werden. Möglicherweise müssen Verfahrensweisen zum Umgang mit gerichtlichen Aufforderungen bezüglich des Zugriffs auf kryptographische Schlüssel in Betracht gezogen werden. So kann es erforderlich sein, verschlüsselte Daten in unverschlüsselter Form als Beweismittel für eine Gerichtsverhandlung verfügbar zu machen.

11 Schutz vor physischem Zugang und Umwelteinflüssen

11.1 Sicherheitsbereiche

Zielsetzung: Verhinderung des nicht autorisierten physischen Zugriffs sowie die Beschädigung und Beeinträchtigung von Daten und informationsverarbeitenden Einrichtungen der Organisation.

11.1.1 Physische Sicherheitszonen

Maßnahme

Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitszonen festgelegt und verwendet werden.

Umsetzungshinweise

Die folgenden Leitlinien sollten ggf. in physischen Sicherheitszonen in Betracht gezogen und umgesetzt werden:

a) Die Sicherheitszonen sollten festgelegt werden, wobei Ort und Sicherungsumfang der einzelnen Zonen von den Sicherheitsanforderungen hinsichtlich der Werte, die sich in der Zone befinden, sowie den Ergebnissen einer Risikoeinschätzung abhängen sollten;

b) Die Zonen in einem Gebäude oder an einem Standort, in denen sich Einrichtungen zur Verarbeitung von Informationen befinden, sollten physisch einwandfrei sein (d. h. es sollten sich keine Lücken in Zonen oder Bereichen befinden, in denen es leicht zu einem Einbruch kommen könnte). Die äußere Bedachung, die Wände und der Bodenbelag des Standorts sollten stabil gebaut sein, und alle Außentüren sollten ausreichend mit Hilfe von Kontrollmechanismen (z. B. Schranken, Alarmvorrichtungen, Verriegelungen usw.) vor unbefugtem Zutritt geschützt sein. Unbewachte Türen und Fenster sollten verriegelt werden, und für Fenster, insbesondere im Erdgeschoss, sollten externe Sicherungseinrichtungen in Betracht gezogen werden;

c) Es sollte ein mit Personal besetzter Empfangsbereich oder dergleichen eingerichtet werden, um den physischen Zugang zum Standort bzw. Gebäude zu kontrollieren. Der Zutritt zu Standorten und Gebäuden sollte nur autorisierten Mitarbeitern gestattet werden;

d) Es sollten ggf. physische Barrieren errichtet werden, um den Zutritt unbefugter Personen und eine Beeinträchtigung der Umwelt zu verhindern;

e) Alle Brandschutztüren in einer Sicherheitszone sollten über Alarmvorrichtungen verfügen sowie überwacht und im Zusammenhang mit den Wänden überprüft werden, um sicherzustellen, dass sie der nach regionalen, nationalen und internationalen Normen erforderlichen Feuerwiderstandsklasse entsprechen. Ein ausfallsicherer Betrieb entsprechend den örtlichen Brandschutzbestimmungen sollte sichergestellt sein;

f) Es sollten geeignete, regionalen, nationalen oder internationalen Normen entsprechende Einbruchmeldeanlagen installiert und regelmäßig überprüft werden, mit denen sich alle Außentüren und alle zugänglichen Fenster überwachen lassen. Ungenutzte Bereiche sollten rund um die Uhr mit Alarmvorrichtungen gesichert werden. Die Sicherung sollte sich auch auf andere Bereiche wie z. B. Computerräume oder Besprechungsräume erstrecken;

g) Der Organisation unterstehende Einrichtungen zur Informationsverarbeitung sollten physisch von jenen Einrichtungen getrennt sein, die von externen Parteien verwaltet werden.

Weitere Informationen

Ein physischer Schutz kann durch Errichtung einer oder mehrerer physischer Barrieren am Gelände der Organisation und den Einrichtungen zur Informationsverarbeitung erreicht werden. Die Verwendung mehrerer Barrieren bietet zusätzlichen Schutz, da der Ausfall einer Barriere keine unmittelbare Beeinträchtigung der Sicherheit zur Folge hat.

Bei einem Sicherheitsbereich kann es sich um ein abschließbares Büro handeln oder um mehrere Räume, die von einer durchgehenden, internen physischen Barriere umgeben sind. Zusätzliche Barrieren und Zonen zur Kontrolle des physischen Zugangs sind möglicherweise erforderlich zwischen Bereichen mit unterschiedlichen Sicherheitsanforderungen innerhalb der Sicherheitszone. Besondere Aufmerksamkeit hinsichtlich der Sicherung des physischen Zugangs sollte Gebäuden geschenkt werden, in denen sich Werte mehrerer Organisationen befinden.

Die Anwendung physischer Zugangskontrollen sollte insbesondere in den Sicherheitsbereichen an die technischen und wirtschaftlichen Bedingungen der Organisation angepasst werden, die in der Risikoeinschätzung dargelegt sind.

11.1.2 Physische Zugangskontrollen

Maßnahme

Sicherheitsbereiche sollten durch angemessene Zugangskontrollen geschützt werden, durch die sichergestellt ist, dass nur autorisiertes Personal Zugang hat.

Umsetzungshinweise

Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) An- und Abmeldung von Besuchern sollten mit Datum und Uhrzeit vermerkt werden, und alle Besucher sollten kontrolliert werden, sofern ihr Aufenthalt nicht zuvor genehmigt wurde. Besuchern sollte der Zutritt nur für spezifische, genehmigte Zwecke gestattet werden, und sie sollten bezüglich der Sicherheitsanforderungen im betreffenden Bereich sowie der Notfallmaßnahmen eingewiesen werden. Die Identität der Besucher sollte auf geeignete Weise bestätigt werden;

b) Der Zugang zu Bereichen, in denen vertrauliche Informationen verarbeitet oder gespeichert werden, sollte mittels geeigneter Zugangskontrollen wie z. B. eines aus einer Zugangskarte und einer geheimen PIN bestehenden Zwei-Faktor-Authentifizierungsmechanismus autorisierten Personen vorbehalten werden;

c) Es sollten ein physisches Protokollbuch oder ein elektronischer Prüfpfad existieren, die sicher aufbewahrt und überwacht werden;

d) Alle Mitarbeiter, Auftragnehmer und externen Parteien sollten dazu verpflichtet werden, eine gut sichtbare Kennzeichnung zu tragen und unverzüglich das Sicherheitspersonal zu benachrichtigen, wenn sie auf unbegleitete Besucher oder Personen treffen, die keine erkennbare Kennzeichnung tragen;

e) Mitarbeitern externer Support-Dienstleister sollte nur dann beschränkter Zugang zu Sicherheitsbereichen oder Einrichtungen zur Verarbeitung vertraulicher Informationen gewährt werden, wenn dies erforderlich ist. Dieser Zugang sollte eigens genehmigt und überwacht werden;

f) Zugangsrechte in Bezug auf Sicherheitsbereiche sollten regelmäßig überprüft und aktualisiert sowie, sofern erforderlich, wieder entzogen werden (siehe 9.2.4 und 9.2.5).

11.1.3 Sicherung von Büros, sonstigen Räumen und Einrichtungen

Maßnahme

Es sind physische Sicherungsvorkehrungen für Büros, sonstige Räume und Einrichtungen zu konzipieren und anzuwenden.

Umsetzungshinweise

Die folgenden Leitlinien sollten bei der Sicherung von Büros, sonstigen Räumen und Einrichtungen beachtet werden:

a) Wichtige Einrichtungen sollten sich in Bereichen befinden, die der Öffentlichkeit normalerweise nicht zugänglich sind;

b) Die Gebäude sollten unauffällig aussehen und möglichst keinen Aufschluss über ihren Zweck geben, keine auffälligen Kennzeichen an der Fassade oder im Inneren aufweisen und keinen Hinweis auf das Vorhandensein von Aktivitäten zur Informationsverarbeitung geben;

c) Die Einrichtungen sollten so konfiguriert sein, dass von außen keine vertraulichen Informationen oder Aktivitäten zu sehen oder zu hören sind. Gegebenenfalls sollte auch eine elektromagnetische Abschirmung in Betracht gezogen werden;

d) Verzeichnisse und interne Telefonbücher, denen die Standorte von Einrichtungen zu entnehmen sind, in denen vertrauliche Informationen verarbeitet werden, sollten ausschließlich autorisierten Personen zugänglich sein.

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Maßnahme

Es sollten physische Schutzvorkehrungen gegen Naturkatastrophen, vorsätzliche Angriffe oder Unfälle konzipiert und angewendet werden.

Umsetzungshinweise

Es sollte eine fachliche Beratung in Anspruch genommen werden, um Schäden aufgrund von Bränden, Überschwemmungen, Erdbeben, Explosionen, Unruhen und anderen Formen von Naturkatastrophen und vom Menschen verursachten Katastrophen zu verhindern.

11.1.5 Arbeit in Sicherheitsbereichen

Maßnahme

Es sollten Verfahren für die Arbeit in Sicherheitsbereichen konzipiert und angewendet werden.

Umsetzungshinweise

Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) Die Mitarbeiter sollten nur im Bedarfsfall über die Existenz eines Sicherheitsbereichs bzw. dort stattfindende Aktivitäten unterrichtet werden;

b) Aus Sicherheitsgründen und zur Unterbindung böswilliger Handlungen sollten unbeaufsichtigte Tätigkeiten in Sicherheitsbereichen vermieden werden;

c) Ungenutzte Sicherheitsbereiche sollten unter Verschluss gehalten und regelmäßig überprüft werden;

d) Das Mitführen von Foto-, Video-, Audio- und sonstigen Aufzeichnungsgeräten wie Mobiltelefonen mit Kameras sollte untersagt und nur mit ausdrücklicher Genehmigung gestattet werden.

Die Vorkehrungen für Arbeiten in Sicherheitsbereichen sollten Kontrollen der Mitarbeiter und externen Benutzer umfassen und alle Aktivitäten umfassen, die im Sicherheitsbereich stattfinden.

11.1.6 Anlieferungs- und Ladezonen

Maßnahme

Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich nicht autorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, sollten kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um nicht autorisierten Zugriff zu verhindern.

Umsetzungshinweise

Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) Der Zugang zu einer Anlieferungs- und Ladezone von außerhalb des Gebäudes sollte nur identifizierten und autorisierten Mitarbeitern ermöglicht werden;

b) Die Anlieferungs- und Ladezone sollte so beschaffen sein, dass Waren beladen und entladen werden können, ohne dass das Lieferpersonal Zugang zu anderen Teilen des Gebäudes erhält;

c) Die Außentüren einer Anlieferungs- und Ladezone sollten gesichert werden, wenn die Innentüren geöffnet sind;

d) Eingehendes Material sollte geprüft und auf Sprengstoffe, Chemikalien und andere Gefahrstoffe untersucht werden, bevor es aus der Anlieferungs- und Ladezone entfernt wird;

e) Eingehendes Material sollte entsprechend den Wertemanagementverfahren (siehe 8) beim Eingang am Standort registriert werden;

f) Eingehende und ausgehende Lieferungen sollten nach Möglichkeit physisch getrennt werden;

g) Eingehende Materialien sollten auf Manipulationen während des Transports untersucht werden. Sofern sich Anzeichen für Manipulationen finden, sollten diese unverzüglich dem Sicherheitspersonal gemeldet werden.

11.2 Sicherheit von Betriebsmitteln

Zielsetzung: Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit.

11.2.1 Platzierung und Schutz von Betriebsmitteln

Maßnahme

Betriebsmittel sollten so platziert und geschützt werden, dass Risiken durch Umweltbedrohungen und Gefährdungen sowie Möglichkeiten für den nicht autorisierten Zugriff verringert werden.

Umsetzungshinweise

Zum Schutz von Betriebsmitteln sollten die folgenden Leitlinien berücksichtigt werden:

a) Die Betriebsmittel sollten so platziert werden, dass ein nicht notwendiger Zugang zu den Arbeitsbereichen möglichst vermieden wird;

b) Der Standort von Einrichtungen zur Informationsverarbeitung, in denen mit sensiblen Daten umgegangen wird, sollte sorgfältig gewählt werden, um das Risiko zu verringern, dass nicht autorisierte Personen während der Verarbeitung Einblick in die Informationen erhalten;

c) Einrichtungen zur Speicherung von Daten sollten vor unberechtigtem Zutritt gesichert werden;

d) Besonders schutzbedürftige Objekte sollten abgesichert werden, um die allgemein erforderliche Schutzstufe reduzieren zu können;

e) Es sollten Maßnahmen ergriffen werden, um das Risiko möglicher physischer oder umweltbezogener Bedrohungen wie z. B. Diebstahl, Feuer, Sprengstoff, Rauch, Wasser (oder Ausfall der Wasserversorgung), Staub, Vibrationen, chemische Auswirkungen, Störungen der Stromversorgung und Telekommunikationseinrichtungen, elektromagnetische Strahlung und Vandalismus möglichst gering zu halten;

f) Es sollten Leitlinien für das Essen, Trinken und Rauchen in der Nähe von Einrichtungen zur Informationsverarbeitung aufgestellt werden;

g) Umweltbedingungen wie Temperatur und Luftfeuchtigkeit sollten auf Bedingungen überwacht werden, die den Betrieb der Einrichtungen zur Informationsverarbeitung beeinträchtigen könnten;

h) Alle Gebäude sollten mit Blitzschutzeinrichtungen ausgestattet werden, und alle eingehenden Strom- und Telekommunikationsleitungen sollten mit Blitzschutzfiltern ausgestattet werden;

i) Bei Betriebsmitteln in industriellen Umgebungen sollte die Anwendung besonderer Schutzmaßnahmen wie Folientastaturen in Betracht gezogen werden;

j) Betriebseinrichtungen, in denen vertrauliche Informationen verarbeitet werden, sollten dergestalt geschützt werden, dass das Risiko von Informationsverlusten aufgrund elektromagnetischer Abstrahlung möglichst gering ist.

11.2.2 Versorgungseinrichtungen

Maßnahme

Betriebsmittel sollten vor Stromausfällen und anderen Betriebsunterbrechungen durch Ausfälle von Versorgungseinrichtungen geschützt werden.

Umsetzungshinweise

Versorgungseinrichtungen (z. B, Elektrizität, Telekommunikation, Wasserversorgung, Gas, Abwasserkanäle, Belüftung und Klimaanlage) sollten sich durch folgende Merkmale auszeichnen:

a) Sie sollten den Spezifikationen des Herstellers der Einrichtungen sowie den vor Ort geltenden gesetzlichen Vorschriften entsprechen;

b) Sie sollten regelmäßig auf ihre ausreichende Auslegung hinsichtlich steigender geschäftlicher Anforderungen sowie ihrer Interaktion mit den anderen Versorgungseinrichtungen begutachtet werden;

c) Sie sollten regelmäßig untersucht und geprüft werden, um ihre ordnungsgemäße Funktion sicherzustellen;

d) Sie sollten bei Bedarf mit Alarmvorrichtungen versehen werden, damit Fehlfunktionen schnell erkannt werden;

e) Sie sollten bei Bedarf mehrere Zuführungen über unterschiedliche Zuleitungswege besitzen.

Eine Notbeleuchtung und ein Notrufsystem sollten vorhanden sein. Die Notschalter und Notventile zur Abschaltung der Strom-, Wasser-, Gas- und anderer Versorgungseinrichtungen sollten sich in der Nähe der Notausgänge oder Geräteräume befinden.

Weitere Informationen

Zusätzliche redundante Netzanschlüsse können mittels mehrfacher Leitungsführungen von mehr als einem Anbieter realisiert werden.

11.2.3 Sicherheit der Verkabelung

Maßnahme

Stromversorgungs- und Telekommunikationskabel, die zur Übertragung von Daten oder zur Unterstützung von Informationsdiensten verwendet werden, sollten vor dem Abfangen der Daten sowie vor Beeinträchtigung oder Beschädigung geschützt werden.

Umsetzungshinweise

Die folgenden Leitlinien zur Verkabelung sollten dabei berücksichtigt werden:

a) Stromversorgungs- und Telekommunikationskabel, die in die Einrichtungen zur Informationsverarbeitung führen, sollten sich möglichst unterirdisch befinden oder auf andere Weise angemessen geschützt sein;

b) Die Stromleitungen sollten von den Telekommunikationsleitungen getrennt sein, um Interferenzen zu verhindern;

c) Bei sensiblen oder betriebswichtigen Systemen sollten folgende weitergehende Maßnahmen ergriffen werden:

   1) Installation von Panzerrohren und verschlossenen Räumen oder Kästen an Untersuchungs- und Endpunkten;

   2) Verwendung elektromagnetischer Abschirmung zum Schutz der Kabel;

   3) Einführung technischer Sweeps und physischer Untersuchungen von nicht autorisierten Geräten, die an die Kabel angeschlossen sind;

   4) kontrollierter Zugang zu Schalttafeln und Kabelräumen.

11.2.4 Instandhaltung von Betriebsmitteln

Maßnahme

Die Betriebsmittel sollten ordnungsnach instand gehalten und gepflegt werden, um ihre Verfügbarkeit und Integrität sicherzustellen.

Umsetzungshinweise

Die folgenden Leitlinien zur Wartung von Betriebsmitteln sollten dabei berücksichtigt werden:

a) Die Betriebsmittel sollten entsprechend den empfohlenen Serviceintervallen und Spezifikationen des Lieferanten gewartet werden;

b) Reparaturen und Wartungsarbeiten sollten ausschließlich von autorisierten Mitarbeitern durchgeführt werden;

c) Alle vermuteten und tatsächlichen Fehler sowie alle vorbeugenden und Korrekturmaßnahmen sollten dokumentiert werden;

d) Wenn Betriebsmittel zur Wartung vorgesehen ist, sollten geeignete Maßnahmen unter Berücksichtigung der Tatsache umgesetzt werden, ob diese Wartung von Mitarbeitern vor Ort oder von Externen durchgeführt wird. Vertrauliche Informationen sollten ggf. von den Betriebsmitteln entfernt werden, oder das Wartungspersonal sollte ausreichende Befugnis erhalten;

e) Es sollten alle durch Versicherungspolicen auferlegten Wartungsanforderungen erfüllt werden;

f) Vor der Wiederinbetriebnahme von Betriebsmitteln nach der Wartung sollte diese untersucht werden, um sicherzustellen, dass sie nicht manipuliert wurde und keine Fehlfunktionen zu befürchten sind.

11.2.5 Entfernung von Werten

Maßnahme

Ausrüstung, Informationen oder Software sollten nicht ohne vorherige Autorisierung vom Standort entfernt werden.

Umsetzungshinweise

Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) Mitarbeiter und externe Benutzer, die befugt sind, die Entfernung von Werten vom Standort anzuordnen, sollten entsprechend benannt werden;

b) Es sollten zeitliche Grenzen für die Entfernung von Werten festgesetzt und Rückgaben auf Konformität überprüft werden;

c) Werte sollten, sofern erforderlich und angemessen, als vom Standort entfernt ausgetragen und bei Rückgabe entsprechend vermerkt werden;

d) Identität, Funktion und Zugehörigkeit aller Personen, die mit den Werten umgehen oder sie verwenden, sollten dokumentiert werden, und diese Aufzeichnungen sollten zusammen mit der Ausrüstung, Information oder Software zurückgegeben werden.

Weitere Informationen

Stichprobenprüfungen, die zur Überprüfung auf eine nicht autorisierte Entfernung von Werten durchgeführt werden, können auch zur Überprüfung auf nicht genehmigte Aufzeichnungsgeräte, Waffen usw. verwendet werden sowie um zu verhindern, dass diese auf den Standort gelangen oder ihn verlassen. Diese Stichprobenprüfungen sollten entsprechend den geltenden Gesetzen und Vorschriften durchgeführt werden. Alle betroffenen Personen sollten erfahren, dass Stichprobenprüfungen durchgeführt werden, und die Überprüfungen sollten nur mit einer den gesetzlichen und amtlichen Vorgaben entsprechenden Befugnis erfolgen.

11.2.6 Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude

Maßnahme

Sicherheitsvorkehrungen sollten unter Berücksichtigung der diversen Risiken bei Arbeiten außerhalb der Betriebsgebäude der Organisation auch auf Werte außerhalb des Standorts angewandt werden.

Umsetzungshinweise

Jede Nutzung von Einrichtungen zur Speicherung und Verarbeitung von Informationen außerhalb der Betriebsgebäude der Organisation sollten vom Management genehmigt werden. Dies gilt für Betriebsmittel im Eigentum der Organisation ebenso wie für Betriebsmittel in Privatbesitz, die im Namen der Organisation genutzt werden.

Zum Schutz von Einrichtungen außerhalb des Standorts sollten die folgenden Leitlinien in Betracht gezogen werden:

a) Betriebsmittel und Medien, die das Betriebsgelände verlassen, sollten in der Öffentlichkeit nicht unbeaufsichtigt gelassen werden;

b) Die Herstelleranweisungen zum Schutz der Betriebsmittel sollten jederzeit beachtet werden. Dies betrifft z. B. den Schutz vor starken elektromagnetischen Feldern;

c) Auf Grundlage einer Risikoeinschätzung sollten Maßnahmen für Bereiche außerhalb des Betriebsgeländes wie Heimarbeitsplätze, Telearbeit und temporäre Standorte festgelegt und geeignete Kontrollmaßnahmen angewendet werden wie z. B. abschließbare Aktenschränke, Grundsatz des aufgeräumten Schreibtisches, Zugriffskontrollen für Computer und sichere Kommunikation mit dem Büro (siehe auch ISO/IEC 27033 zur Netzwerksicherheit);

d) Wenn Betriebsmittel außerhalb des Betriebsgeländes zwischen verschiedenen Personen oder externen Parteien weitergegeben werden, sollte ein Protokoll geführt werden, in dem die Kontrollkette für die Betriebsmittel einschließlich mindestens der Namen und Organisationen der für die Betriebsmittel Verantwortlichen festgehalten werden.

Risiken, z. B. Beschädigung, Diebstahl oder Abhören, können an verschiedenen Orten sehr unterschiedlich stark ausgeprägt sein und sollten bei der Bestimmung der am besten geeigneten Kontrollmaßnahmen in Betracht gezogen werden.

Weitere Informationen

Als Betriebsmittel zur Speicherung und Verarbeitung zählen alle Arten von Personalcomputern, Organizern, Mobiltelefonen, Smartcards, Papier oder andere Medien, die für Heimarbeit verwendet oder aus dem normalen Arbeitsumfeld gebracht werden.

Weitere Informationen zu anderen Aspekten des Schutzes mobiler Betriebsmittel können 6.2 entnommen werden.

Es kann angemessen sein, das Risiko dadurch zu vermeiden, dass bestimmten Mitarbeitern von einer Tätigkeit außerhalb des Betriebsgeländes abgeraten oder ihre Nutzung portabler IT-Ausrüstung beschränkt wird.

11.2.7 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln

Maßnahme

Alle Betriebsmittel, die Speichermedien beinhalten, sollten vor ihrer Entsorgung oder Wiederverwendung überprüft werden, um sicherzustellen, dass vertrauliche Daten und lizenzierte Software entfernt oder sicher überschrieben wurden.

Umsetzungshinweise

Vor der Entsorgung oder Wiederverwendung sollten Betriebsmittel überprüft werden, um herauszufinden, ob sie Speichermedien enthalten.

Speichermedien, die vertrauliche oder urheberrechtlich geschützte Informationen enthalten, sollten anstelle der Anwendung der standardmäßigen Lösch- oder Formatierungsfunktion physisch zerstört oder die Informationen sollten mittels geeigneter Verfahren dergestalt zerstört, gelöscht oder überschrieben werden, dass die ursprünglichen Informationen nicht wiederhergestellt werden können.

Weitere Informationen

Beschädigte Betriebsmittel, die Datenträger beinhalten, müssen möglicherweise einer Risikoeinschätzung unterzogen werden, um zu bestimmen, ob diese Datenträger physisch zerstört, zur Reparatur versandt oder anderweitig ausgesondert werden sollten. Durch fahrlässige Entsorgung bzw. Wiederverwendung der Betriebsmittel können Informationen in die Hände Unbefugter geraten.

Zusätzlich zur sicheren Datenträgerlöschung lässt sich durch Gesamtverschlüsselung des Datenträgers das Risiko einer Offenlegung vertraulicher Informationen bei der Entsorgung oder Wiederverwendung von Betriebsmitteln unter folgenden Voraussetzungen verringern:

a) Das Verschlüsselungsverfahren ist stark genug und umfasst tatsächlich den gesamten Datenträger (einschließlich Schlupfspeicher, Auslagerungsdateien usw.);

b) Die verwendeten Schlüssel sind lang genug, um Brute-Force-Angriffen standzuhalten;

c) Die verwendeten Schlüssel werden ihrerseits sicher aufbewahrt (und z. B. auf keinen Fall auf demselben Datenträger gespeichert).

Weitere Empfehlungen zur Verschlüsselung können Abschnitt 10 entnommen werden.

Die Verfahren zum sicheren Überschreiben von Speichermedien sind je nach Technologie des Speichermediums unterschiedlich. Werkzeuge zum Überschreiben sollten überprüft werden, um sicherzustellen, dass sie für die jeweilige Speichermedientechnologie geeignet sind.

11.2.8 Unbeaufsichtigte Endgeräte

Maßnahme

Die Benutzer müssen sicherstellen, dass unbeaufsichtigte Endgeräte angemessen geschützt sind.

Umsetzungshinweise

Allen Benutzern müssen die Sicherheitsanforderungen und -verfahren zum Schutz unbeaufsichtigter Endgeräte sowie ihre Zuständigkeiten bei der Umsetzung dieses Schutzes bekannt sein. Die Benutzer sollten angewiesen werden, die folgenden Grundsätze zu beachten:

a) Nach Abschluss einer Tätigkeit müssen aktive Sitzungen beendet werden, sofern sie nicht mittels eines geeigneten Sperrmechanismus, z. B. eines kennwortgeschützten Bildschirmschoners, gesichert werden können;

b) Die Benutzer sollten sich von nicht mehr benötigten Netzwerkdiensten abmelden;

c) Nicht genutzte Computer oder Mobilgeräte sind mittels einer Tastensperre oder einer anderen geeigneten Maßnahme wie z. B. der Abfrage eines Kennworts vor nicht autorisiertem Zugriff zu sichern.

11.2.9 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

Maßnahme

Der Grundsatz des aufgeräumten Schreibtisches für Papiere und Wechselmedien sowie des leeren Bildschirms für informationsverarbeitende Einrichtungen sollte Anwendung finden.

Umsetzungshinweise

Beim Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms sollten die Klassifizierungen von Informationen (siehe 8.2), die gesetzlichen und vertraglichen Anforderungen (siehe 18.1) und die entsprechenden Risiken und kulturellen Aspekte der Organisation Berücksichtigung finden. Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) Sensible und geschäftskritische Informationen, z. B. auf Papier oder elektronischen Speichermedien, sollten unter Verschluss gehalten werden (idealerweise in einem Safe oder Schrank oder anderen Sicherheitsmöbeln), wenn sie nicht benötigt werden, insbesondere dann, wenn das Büro nicht besetzt ist;

b) Computer und Terminals sollten erst nach Abmeldung verlassen werden oder mit einer Bildschirm- und Tastensperre geschützt sein, die durch ein Kennwort, ein Token oder einen ähnlichen Mechanismus zur Benutzerauthentifizierung gesichert ist, wenn sie unbeaufsichtigt sind, sowie bei Nichtnutzung durch eine Tastatursperre, Kennwörter oder andere Maßnahmen geschützt sind;

c) Die nicht autorisierte Nutzung von Fotokopierern und anderen Vervielfältigungstechnologien (z. B. Scanner, Digitalkameras) sollte verhindert werden;

d) Papiere, die sensible oder zugangsbeschränkte Informationen enthalten, sollten unverzüglich aus dem Drucker entfernt werden.

Weitere Informationen

Durch den Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms verringern sich die Risiken eines nicht autorisierten Zugriffs auf sowie den Verlust und die Beschädigung von Informationen während und außerhalb der üblichen Arbeitszeiten. Safes und andere Formen sicherer Lagerungseinrichtungen können außerdem dorthin verbrachte Informationen vor Katastrophen wie Bränden, Erdbeben, Überschwemmungen oder Explosionen schützen.

Die Nutzung von Druckern mit Pincode-Funktion sollte in Betracht gezogen werden, um sicherzustellen, dass nur die jeweiligen Urheber ihre Ausdrucke erhalten können und nur dann, wenn sie neben dem Drucker stehen.

12 Betriebssicherheit

12.1 Betriebsverfahren und Zuständigkeiten

Zielsetzung: Sicherstellung des ordnungsnachen und sicheren Betriebs von Einrichtungen zur Informationsverarbeitung.

12.1.1 Dokumentierte Betriebsverfahren

Maßnahme

Die Betriebsverfahren sollten dokumentiert und allen Benutzern zugänglich gemacht werden, die sie benötigen.

Umsetzungshinweise

Es sollten dokumentierte Verfahren für betriebliche Aktivitäten im Zusammenhang mit informationsverarbeitenden und Telekommunikationseinrichtungen vorbereitet werden, wie z. B. zum Hoch- und Herunterfahren der Computer, zum Backup, zur Wartung von Betriebsmitteln, zum Umgang mit Medien sowie zur Verwaltung und Sicherheit der Computerräume und des Umgangs mit E-Mails.

In den Betriebsverfahren sollten die Betriebsanweisungen u. a. zu den folgenden Punkten spezifiziert sein:

a) Installation und Konfiguration der Systeme;

b) Verarbeitung von und Umgang mit Informationen (automatisiert und manuell);

c) Backup (siehe 12.3);

d) Planungsanforderungen, einschließlich gegenseitiger Abhängigkeiten mit anderen Systemen, frühestmöglichem Arbeitsbeginn und spätestmöglicher Fertigstellungstermine;

e) Anweisungen zum Umgang mit Fehlern und anderen außergewöhnlichen Umständen, die während der Arbeitsausführung entstehen können, einschließlich Beschränkungen bezüglich der Nutzung von Dienstprogrammen (siehe 9.4.4);

f) Ansprechpartner für Support und Eskalation einschließlich der Ansprechpartner für den Support bei unerwarteten betrieblichen oder technischen Schwierigkeiten;

g) besondere Anweisungen für die Ausgabe und den Umgang mit Medien wie z. B. die Nutzung besonderen Büropapiers oder die Verwaltung vertraulicher Ausgabedaten einschließlich Verfahren zur sicheren Entsorgung der Ausgabedaten fehlgeschlagener Jobs (siehe 8.3 und 11.2.7);

h) Verfahren für System-Neustart und Wiederherstellung zur Nutzung bei einem Systemausfall;

i) die Verwaltung von Prüfpfad- und Systemprotokoll-Informationen (siehe 12.4);

j) Überwachungsverfahren (siehe 12.4).

Die Betriebsverfahren und die dokumentierten Verfahren für Systemaktivitäten sollten wie offizielle Dokumente behandelt werden, und Änderungen sollten einer Genehmigung durch das Management bedürfen. Informationssysteme sollten, sofern dies technisch durchführbar ist, zentral mittels derselben Verfahren, Werkzeuge und Dienstprogramme verwaltet werden.

12.1.2 Änderungsmanagement

Maßnahme

Änderungen in der Organisation, an Geschäftsprozessen, an Datenverarbeitungseinrichtungen und an Systemen, die Einfluss auf die Informationssicherheit haben, sollten kontrolliert werden.

Umsetzungshinweise

Die folgenden Punkte sollten dabei insbesondere berücksichtigt werden:

a) Feststellung und Protokollierung wesentlicher Änderungen;

b) Planung und Prüfung von Änderungen;

c) Beurteilung der möglichen Auswirkungen derartiger Änderungen, einschließlich der Auswirkungen auf die Informationssicherheit;

d) formelles Genehmigungsverfahren für vorgeschlagene Änderungen;

e) Sicherstellung, dass die Anforderungen an die Informationssicherheit erfüllt wurden;

f) Kommunizierung von Änderungsdetails an alle relevanten Personen;

g) Alternativverfahren, darunter Verfahren und Zuständigkeiten, um bei nicht erfolgreichen Änderungen und unvorhergesehenen Ereignissen den Vorgang abzubrechen und die Änderungen rückgängig zu machen;

h) Bereitstellung eines Änderungsprozesses für den Notfall, um die schnelle und kontrollierte Umsetzung von Änderungen zur Behebung eines Vorfalls (siehe 16.1) zu ermöglichen.

Es sollten formelle Verantwortungsbereiche und Verfahren für das Management existieren, um die zufriedenstellende Kontrolle aller Änderungen sicherzustellen. Wenn Änderungen vorgenommen werden, sollte ein Audit-Protokoll erstellt werden, das alle relevanten Informationen enthält.

Weitere Informationen

Die unzureichende Kontrolle von Änderungen an Einrichtungen und Systemen zur Informationsverarbeitung ist eine häufige Ursache von System- oder Sicherheitsausfällen. Änderungen an der Betriebsumgebung, insbesondere beim Übergang eines Systems von der Entwicklungs- in die Betriebsphase, kann Einfluss auf die Zuverlässigkeit der Anwendungen (siehe 14.2.2) haben.

12.1.3 Kapazitätsmanagement

Maßnahme

Die Ressourcennutzung sollte überwacht und abgestimmt werden, und es sind Prognosen zu zukünftigen Kapazitätsanforderungen zu erstellen, um eine ausreichende Systemleistung sicherzustellen.

Umsetzungshinweise

Die Kapazitätsanforderungen sollten unter Berücksichtigung der Betriebswichtigkeit des betroffenen Systems festgestellt werden. Es sollte eine Abstimmung und Überwachung des Systems erfolgen, um die Verfügbarkeit der Systeme sicherzustellen und ggf. zu verbessern. Es sollten Kontrollen eingerichtet werden, mit denen Probleme rechtzeitig erkannt werden. Bei Prognosen zu zukünftigen Kapazitätsanforderungen sollten neue geschäftliche und systembezogene Anforderungen sowie aktuelle und zukünftige Trends bezüglich der informationsverarbeitenden Einrichtungen der Organisation in Betracht gezogen werden.

Besondere Aufmerksamkeit muss Ressourcen mit langen Vorlaufzeiten bei der Bereitstellung oder hohen Kosten geschenkt werden. Daher sollten die Manager die Nutzung wichtiger Systemressourcen überwachen. Sie sollten Nutzungstrends angeben, insbesondere im Verhältnis zu Geschäftsanwendungen oder den Verwaltungstools der Informationssysteme.

Die Manager sollten diese Information nutzen, um mögliche Engpässe und Abhängigkeiten von Mitarbeitern in Schlüsselpositionen festzustellen und zu vermeiden, die eine Bedrohung für die Systemsicherheit oder die Dienste darstellen könnte, und entsprechende Maßnahmen zu planen.

Die Bereitstellung einer ausreichenden Kapazität kann durch Steigerung der Kapazität oder Verringerung des Bedarfs erreicht werden. Beispiele für die Kapazitätsverwaltung:

a) Löschung veralteter Daten (Speicherplatz);

b) Außerbetriebnahme von Anwendungen, Systemen, Datenbanken oder Umgebungen;

c) Optimierung von Batch-Prozessen und -Planung;

d) Optimierung von Anwendungslogik oder Datenbankabfragen;

e) Verweigerung von oder Begrenzung der Bandbreite für ressourcenintensive Dienste, die nicht geschäftskritisch sind (z. B. Video-Streaming).

Bei erfolgskritischen Systemen sollte die Aufstellung eines dokumentierten Kapazitätsmanagementplans in Betracht gezogen werden.

Weitere Informationen

Diese Maßnahme bezieht sich neben Büros und Einrichtungen auch auf die Personalkapazität.

12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Maßnahme

Entwicklungs-, Test- und Betriebsumgebungen sollten getrennt werden, um das Risiko nicht autorisierter Zugriffe oder nicht autorisierter Änderungen an der Betriebsumgebung zu verringern.

Umsetzungshinweise

Nachdem festgestellt wurde, wie stark Betriebs-, Test- und Entwicklungsumgebung zur Verhinderung von Problemen im Betriebsablauf voneinander getrennt werden müssen, sollte diese Trennung umgesetzt werden.

Die folgenden Punkte sollten dabei berücksichtigt werden:

a) Regeln für den Transfer von Software vom Entwicklungs- zum Betriebsstatus sollten festgelegt und dokumentiert werden;

b) Entwicklungs- und Betriebssoftware sollten auf unterschiedlichen Systemen oder Computerprozessoren und in unterschiedlichen Domänen oder Verzeichnissen laufen;

c) Änderungen an betrieblichen Systemen und Anwendungen sollten vor der Anwendung auf die betrieblichen Systeme in einer Prüf- oder Staging-Umgebung getestet werden;

d) Die Tests sollte nur unter außergewöhnlichen Umständen auf den betrieblichen Systemen durchgeführt werden;

e) Der Zugriff aus den betrieblichen Systemen auf Compiler, Editoren und andere Entwicklungswerkzeuge sollte nur dann möglich sein, wenn dies erforderlich ist;

f) Die Benutzer sollten für die betrieblichen und die Testsysteme unterschiedliche Benutzerprofile verwenden, die in den Menüs entsprechend angezeigt werden, um das Risiko eines Fehlers zu verringern;

g) Sensible Daten sollten nicht in das System der Testumgebung kopiert werden, es sei denn, dass entsprechende Kontrollen für das Testsystem zur Verfügung stehen (siehe 14.3).

Weitere Informationen

Entwicklungs- und Testaktivitäten können zu schwerwiegenden Problemen durch z. B. die unbeabsichtigte Veränderung von Dateien oder der Systemumgebung bzw. einen Systemausfall führen. Die Aufrechterhaltung einer bekannten und stabilen Umgebung ist erforderlich, um sinnvolle Überprüfungen durchzuführen und einen unerwünschten Entwicklerzugriff auf die Betriebsumgebung zu verhindern.

Wenn Mitarbeiter aus den Bereichen Entwicklung oder Prüfung Zugriff auf das betriebliche System und dessen Informationen haben, können sie nicht autorisierten und ungeprüften Code einfügen oder die betrieblichen Daten verändern. Bei einigen Systemen könnte diese Möglichkeit dazu missbraucht werden, betrügerische Absichten zu verfolgen oder ungeprüften bzw. Schadcode einzuschleusen, was zu schwerwiegenden Problemen im Betriebsablauf führen kann.

Entwickler und Tester stellen außerdem eine Bedrohung für die Vertraulichkeit der betrieblichen Daten dar. Entwicklungs- und Prüfaktivitäten können zu unbeabsichtigten Veränderungen an der Software oder den Informationen führen, wenn sie in derselben Rechnerumgebung stattfinden. Eine Trennung der Entwicklungs-, der Test- und der Betriebsumgebung ist daher wünschenswert, um das Risiko unbeabsichtigter Veränderungen oder eines nicht autorisierten Zugriffs auf die Betriebssoftware und die Geschäftsdaten zu verringern (zum Schutz der Test-Daten siehe 14.3).

12.2 Schutz vor Malware

Zielsetzung: Sicherstellung, dass Daten und Datenverarbeitungseinrichtungen vor Malware geschützt sind.

12.2.1 Kontrollmaßnahmen gegen Malware

Maßnahme

Es sollten Erkennungs-, Präventions- und Wiederherstellungsmaßnahmen zum Schutz vor Malware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer implementiert werden.

Umsetzungshinweise

Der Malware-Schutz sollte sich auf Malware-Erkennungs- und Reparatur-Software, eine Sensibilisierung für das Thema Informationssicherheit sowie geeignete Kontrollen für den Systemzugriff und das Änderungsmanagement stützen. Die folgenden Leitlinien sollten dabei berücksichtigt werden:

a) Erstellung einer offiziellen Richtlinie, nach der die Nutzung nicht autorisierter Software untersagt ist (siehe 12.6.2 und 14.2.);

b) Umsetzung von Maßnahmen zur Verhinderung bzw. Erkennung der Nutzung nicht autorisierter Software (z. B. Positivliste für Anwendungen);

c) Umsetzung von Maßnahmen zur Verhinderung bzw. Erkennung der Nutzung bekannter oder potenzieller Schadcode-Websites (z. B. Negativliste);

d) Erstellung einer offiziellen Richtlinie zum Schutz vor Risiken unter Angabe zu ergreifender Schutzmaßnahmen im Zusammenhang mit dem Empfang von Dateien und Software, die aus externen Netzwerken stammen oder über diese versendet wurden oder die von einem anderen Medium stammen;

e) Behebung von Schwachstellen, die durch Malware ausgenutzt werden könnten, z. B. durch das Management technischer Schwachstellen (siehe 12.6);

f) Durchführung regelmäßiger Überprüfungen der Software und des Datenbestands von Systemen, die betriebswichtige Geschäftsprozesse unterstützen, wobei das Vorhandensein nicht genehmigter Dateien oder nicht autorisierter Hinzufügungen eine offizielle Untersuchung nach sich ziehen sollte;

g) Installation und regelmäßige Aktualisierung einer Malware-Erkennungs- und Reparatur-Software zum routinemäßigen Scannen von Computern und Medien als Vorsichtsmaßnahme, wobei der Scan folgende Punkte umfassen sollte:

   1) Untersuchung aller über Netzwerke empfangener oder über ein Speichermedium erhaltener Dateien auf Malware vor der Verwendung;

   2) Untersuchung von E-Mail-Anhängen und heruntergeladenen Dateien auf Malware vor der Verwendung, wobei dieser Scan an verschiedenen Stellen erfolgen kann, z. B. auf den E-Mail-Servern, auf den Desktop-Rechnern oder beim Zugang zum Netzwerk der Organisation;

   3) Untersuchung von Websites auf Malware,

h) Festlegung von Verfahren und Verantwortlichkeiten zum Umgang mit dem Malware-Schutz auf den Systemen, zur Nutzungsschulung, zur Berichterstattung über Malware-Angriffe und zu Wiederherstellungsmaßnahmen im Anschluss daran;

i) Vorbereitung entsprechender Geschäftskontinuitätspläne zur Wiederherstellung nach Malware-Angriffen, einschließlich aller erforderlichen Daten, eines Software-Backups und Vorkehrungen für die Wiederherstellung (siehe 12.3);

j) Umsetzung von Verfahren zur regelmäßigen Aktualisierung des eigenen Kenntnisstands, z. B. durch Anmeldung zu Mailing-Listen oder Auswertung von Websites, auf denen über neue Malware informiert wird;

k) Umsetzung von Verfahren zur Verifizierung malwarebezogener Informationen und zur Sicherstellung, dass Warnmeldungen präzise und informativ sind, wobei die Führungskräfte gewährleisten sollten, dass qualifizierte Quellen wie z. B. seriöse Zeitschriften, zuverlässige Internet-Seiten oder Anbieter von Malware-Schutzprogrammen herangezogen werden, um zwischen Falschmeldungen und tatsächlichen Malware-Gefahren unterscheiden zu können und allen Benutzern das Problem von Falschmeldungen bewusst gemacht werden und eine Anleitung zum Umgang mit erhaltenen Meldungen dieser Art gegeben werden sollte;

l) Isolierung von Umgebungen, in denen es zu katastrophalen Auswirkungen kommen könnte.

Weitere Informationen

Die Verwendung von zwei oder mehr Software-Produkten zum Schutz vor Malware innerhalb der Informationsverarbeitungsumgebung, die sich unterschiedlicher Technologien bedienen und von verschiedenen Anbietern stammen, kann die Wirksamkeit des Malware-Schutzes verbessern.

Es sollte sorgfältig darauf geachtet werden, dass es im Rahmen der Wartungs- und Notfallverfahren zu keiner Einschleusung von Malware kommt, die mittels der bestehenden Maßnahmen zum Schutz vor Malware nicht erkannt wird.

Unter bestimmten Bedingungen kann der Malware-Schutz eine Störung in den Betriebsabläufen verursachen.

Die ausschließliche Verwendung von Malware-Erkennungs- und Reparatur-Software als Maßnahme gegen Malware ist meist nicht ausreichend und sollte von Betriebsverfahren zur Verhinderung der Einschleusung von Malware begleitet werden.

12.3 Backup

Zielsetzung: Schutz vor Datenverlust.

12.3.1 Datensicherungen

Maßnahme

Sicherungskopien von Daten und Software sowie System-Images sollten angefertigt und regelmäßig entsprechend einer vereinbarten Sicherungsleitlinie geprüft werden.

Umsetzungshinweise

Es sollte eine Sicherungsleitlinie erstellt werden, in der die Anforderungen der Organisation in Bezug auf die Sicherung von Daten, Software und Systemen festgelegt sind.

In der Sicherungsleitlinie sind außerdem die Aufbewahrungs- und Schutzanforderungen dargelegt.

Es sollten angemessene Sicherungseinrichtungen vorhanden sein, um zu gewährleisten, dass alle wichtigen Informationen und Softwareanwendungen nach einem Schaden oder Medienausfall wiederhergestellt werden können.

Bei der Aufstellung eines Backup-Plans sollten die folgenden Punkte in Betracht gezogen werden:

a) Es sollten genaue und vollständige Aufzeichnungen der Sicherungskopien und der dokumentierten Wiederherstellungsverfahren erstellt werden;

b) Umfang (z. B. komplettes oder differentielles Backup) und Häufigkeit der Sicherungen sollten den geschäftlichen Anforderungen der Organisation, den Sicherheitsanforderungen bezüglich der betreffenden Informationen und der Wichtigkeit der Information für die Fortführung der Betriebstätigkeit entsprechen;

c) Die Sicherungen sollten an einem externen Speicherort in ausreichender Entfernung abgelegt werden, um vor Schäden am Hauptstandort geschützt zu sein;

d) Die Sicherungsinformationen sollten über einen angemessenen Schutz vor physischen und Umweltfaktoren (siehe 11) verfügen, der den am Hauptstandort angewandten Normen entspricht;

e) Die Sicherungsmedien sollten regelmäßig überprüft werden, um sicherzustellen, dass auf sie im Notfall Verlass ist. Dies sollte zusammen mit einer Überprüfung der Wiederherstellungsverfahren in Verbindung mit einer Überprüfung der für die Wiederherstellung benötigten Zeit erfolgen. Bei der Überprüfung der Wiederherstellungsfunktion sollten die gesicherten Daten auf ein separates Prüfmedium zurückgespielt werden, statt das Ursprungsmedium zu überschreiben, um im Fall eines fehlgeschlagenen Sicherungs- oder Wiederherstellungsprozesses eine irreparable Beschädigung oder sogar einen Verlust der Daten zu vermeiden;

f) In Situationen, in denen Vertraulichkeit besonders wichtig ist, sollten die Sicherung mittels Verschlüsselung geschützt werden.

Im Rahmen der Betriebsverfahren sollten die Durchführung von Sicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Sicherungen festlegt werden, um die Vollständigkeit der Backups nach der Sicherungsrichtlinie zu gewährleisten.

Sicherungsvorkehrungen für einzelne Systeme und Dienste sollten regelmäßig überprüft werden, um zu gewährleisten, dass sie die Anforderungen der Geschäftskontinuitätspläne erfüllen. Bei betriebswichtigen Systemen und Diensten sollten die Sicherungsvorkehrungen alle Systeminformationen, -anwendungen und -daten umfassen, die zur Wiederherstellung des kompletten Systems bei einem Schaden erforderlich sind.

Der Aufbewahrungszeitraum für wichtige geschäftliche Informationen sollte unter Berücksichtigung von Anforderungen zur dauerhaften Aufbewahrung von Archivkopien bestimmt werden.

12.4 Protokollierung und Überwachung

Zielsetzung: Aufzeichnung von Ereignissen und Generierung von Beweismaterial.

12.4.1 Ereignisprotokollierung

Maßnahme

Es sollten Ereignisprotokolle angefertigt, aufbewahrt und regelmäßig geprüft werden, in denen Aktivitäten der Benutzer, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden.

Umsetzungshinweise

Die Ereignisprotokolle sollten die folgenden Elemente enthalten (sofern relevant):

a) Benutzerkennungen;

b) Systemaktivitäten;

c) Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. Anmeldung und Abmeldung;

d) Geräteidentität oder -standort (falls möglich) und Systembezeichnung;

e) Aufzeichnung erfolgreicher und abgelehnter Systemzugriffsversuche;

f) Aufzeichnung erfolgreicher und abgelehnter Versuche, auf Daten oder andere Ressourcen zuzugreifen;

g) Änderungen der Systemkonfiguration;

h) Nutzung von Privilegien;

i) Nutzung von Dienstprogrammen und Anwendungen;

j) Dateien, auf die zugegriffen wurde, und Art des Zugriffs;

k) Netzwerkadressen und Protokolle;

l) vom Zugriffskontrollsystem ausgelöste Alarme;

m) Aktivierung und Deaktivierung von Schutzsystemen wie des Virenschutz- und des Angriffserkennungssystems;

n) Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt werden.

Die Ereignisprotokollierung bildet den Grundstein für die automatisierten Überwachungssysteme, die in der Lage sind, konsolidierte Berichte und Warnungen zur Systemsicherheit zu erzeugen.

Weitere Informationen

Ereignisprotokolle können sensible Daten und personenbezogene Informationen enthalten. Daher sollten entsprechende Maßnahmen zum Schutz der Privatsphäre ergriffen werden (siehe 18.1.4).

Die Systemadministratoren sollten möglichst keine Befugnis besitzen, die Protokollierung ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren (siehe 12.4.3).

12.4.2 Schutz von Protokollinformationen

Maßnahme

Protokollierungseinrichtungen und Protokollinformationen sollten vor Manipulation und unbefugtem Zugriff geschützt werden.

Umsetzungshinweise

Die Maßnahmen sollten auf den Schutz vor nicht autorisierten Änderungen der Protokollinformationen und Problemen im Betriebsablauf im Zusammenhang mit der Protokollierungseinrichtung abzielen, darunter:

a) Änderungen der aufgezeichneten Nachrichtentypen;

b) bearbeitete oder gelöschte Protokolldateien;

c) Überschreitung der Speicherkapazität der Protokolldatenträger mit dem Ergebnis, dass Ereignisse nicht mehr aufgezeichnet oder frühere Ereignisse überschrieben werden.

Einige Audit-Protokolle müssen möglicherweise im Rahmen der Aufbewahrungsleitlinie oder aufgrund von Anforderungen zum Sammeln und Speichern von Beweismaterial (siehe 16.1.7) archiviert werden.

Weitere Informationen

Systemprotokolle enthalten häufig eine große Anzahl von Informationen, die vielfach für die Überwachung der Informationssicherheit nicht relevant sind. Zur Ermittlung von Ereignissen, die für die Überwachung der Informationssicherheit von Bedeutung sind, sollte erwogen werden, sich entsprechende Nachrichtentypen automatisch in eine zweite Protokolldatei kopieren zu lassen oder geeignete Dienstprogramme oder Audit-Werkzeuge zur Durchführung einer Dateiabfrage und -rationalisierung zu verwenden.

Die Systemprotokolle müssen geschützt werden, denn falls die Daten verändert oder enthaltene Daten gelöscht werden können, führt dies möglicherweise zu einem falschen Gefühl der Sicherheit. Zum Schutz der Protokolldateien können diese in Echtzeit auf ein System kopiert werden, das sich außerhalb des Verfügungsbereichs eines Systemadministrators oder Betreibers befindet.

12.4.3 Administrator- und Betreiberprotokolle

Maßnahme

Es sollten Protokolle der Aktivitäten von Systemadministratoren und Systembetreibern angefertigt, geschützt und regelmäßig geprüft werden.

Umsetzungshinweise

Inhaber von Benutzerkonten mit Sonderzugangsrechten können möglicherweise die Protokolle von informationsverarbeitenden Einrichtungen manipulieren, die ihnen direkt unterstellt sind. Daher ist es notwendig, die Protokolle zu schützen und zu prüfen, um die Verantwortlichkeit für Benutzer mit Sonderzugangsrechten aufrechtzuerhalten.

Weitere Informationen

Ein Angriffserkennungssystem, das außerhalb des Einflussbereichs der System- und Netzwerkadministratoren verwaltet wird, kann zur Überwachung der Konformität der System- und Netzwerkadministrationsaktivitäten verwendet werden.

12.4.4 Zeitsynchronisation

Maßnahme

Die Uhren aller relevanten Datenverarbeitungssysteme innerhalb einer Organisation oder einer Sicherheitsdomäne sollten auf eine einzelne Referenz-Zeitquelle synchronisiert werden.

Umsetzungshinweise

Die externen und internen Anforderungen für die Zeitdarstellung, -synchronisation und -genauigkeit sollten dokumentiert werden. Bei diesen Anforderungen kann es sich um gesetzliche, behördliche oder vertragliche Vorgaben, einzuhaltende Normen oder Anforderungen zur internen Überwachung handeln. Es sollte eine standardisierte Referenz-Zeit zur Verwendung innerhalb der Organisation festgelegt werden.

Die Herangehensweise der Organisation zur Ermittlung einer Referenz-Zeit aus einer oder mehreren externen Quellen und die Synchronisierungsmethode für die internen Uhren sollten dokumentiert und umgesetzt werden.

Weitere Informationen

Die korrekte Einstellung der Computeruhren ist wichtig, um die Genauigkeit der Audit-Protokolle sicherzustellen, die möglicherweise für Untersuchungen oder als Beweisstück in Rechts- oder Disziplinarfällen benötigt werden. Ungenaue Audit-Protokolle können derartige Untersuchungen behindern und der Glaubwürdigkeit derartiger Beweisstücke schaden. Als Referenzuhr für die Protokollierungssysteme kann eine Uhr verwendet werden, die mit dem gesendeten Zeitsignal einer nationalen Atomuhr verbunden ist. Zur Synchronisation aller Server mit der Referenzuhr kann ein Netzwerkzeit-Protokoll verwendet werden.

12.5 Kontrolle von Betriebssoftware

Zielsetzung: Sicherstellung der Integrität von betrieblichen Systemen.

12.5.1 Installation von Software auf betrieblichen Systemen

Maßnahme

Es sollten Verfahren zur Kontrolle der Installation von Software auf betriebsrelevanten Systemen implementiert werden.

Umsetzungshinweise

Die folgenden Leitlinien sollten zur Änderungskontrolle bei Software auf betrieblichen Systemen beachtet werden:

a) Die Aktualisierung der Betriebssoftware, Anwendungen und Programmbibliotheken sollte nur von geschulten Administratoren auf Grundlage einer entsprechenden Autorisierung durch das Management (siehe 9.4.5) durchgeführt werden;

b) Auf den betrieblichen Systemen sollte sich nur genehmigter, ausführbarer Code befinden, kein Entwicklercode und keine Compiler;

c) Anwendungen und Betriebssystem-Software sollten erst nach umfassenden und erfolgreichen Tests implementiert werden. Die Tests sollten die Aspekte Software-Ergonomie, Sicherheit, Auswirkungen auf andere Systeme und Benutzerfreundlichkeit umfassen und auf separaten Systemen durchgeführt werden (siehe 12.1.4). Es sollte sichergestellt werden, dass alle zugehörigen Programmquellbibliotheken aktualisiert wurden;

d) Es sollte ein Konfigurationskontrollsystem verwendet werden, um die Kontrolle über sämtliche implementierte Software sowie die Systemdokumentation zu gewährleisten;

e) Vor der Umsetzung der Änderungen sollte dafür gesorgt werden, dass eine Rollback-Strategie existiert;

f) Sämtliche Aktualisierungen der Betriebsprogrammbibliotheken sollten in einem Audit-Protokoll festgehalten werden;

g) Frühere Versionen der Anwendungssoftware sollten für den Notfall aufbewahrt werden;

h) Alte Software-Versionen sollten archiviert werden, zusammen mit allen erforderlichen Informationen und Parametern, Verfahren, Konfigurationsdetails und unterstützender Software, solange sich die Daten im Archiv befinden.

Anbietersoftware, die in den betrieblichen Systemen verwendet wird, sollte die vom Lieferanten angebotene Wartung erfahren. Softwareanbieter stellen den Support für ältere Software-Versionen nach einiger Zeit ein. Die Organisation sollte sich mit den Risiken beschäftigen, die mit dem Einsatz einer nicht unterstützten Software verbunden sind.

Bei jeder Entscheidung zur Aktualisierung auf eine neue Version sollten die geschäftlichen Anforderungen für die Änderung und die Sicherheit der Version berücksichtigt werden, z. B. die Einführung neuer Funktionen zur Verbesserung der Informationssicherheit oder Anzahl und Schweregrad der Probleme hinsichtlich der Informationssicherheit, von der diese Version betroffen ist. Software-Patches sollten angewendet werden, wenn sie dazu beitragen, Schwächen hinsichtlich der Informationssicherheit zu beheben oder zu mindern (siehe 12.6).

Physischen oder logischen Zugang sollten nur Lieferanten zu Support-Zwecken erhalten, wenn dies erforderlich ist und vom Management genehmigt wurde. Die Aktivitäten des Lieferanten sollten überwacht werden (siehe 15.2.1).

Die Computersoftware kann von extern beschaffter Softwareanwendungen bzw. Modulen abhängig sein. Diese sollten überwacht und kontrolliert werden, um nicht autorisierte Veränderungen zu verhindern, die zu Sicherheitsschwachstellen führen könnten.

12.6 Technisches Schwachstellenmanagement

Zielsetzung: Verhinderung einer Ausnutzung technischer Schwachstellen.

12.6.1 Management technischer Schwachstellen

Maßnahme

Informationen über technische Schwachstellen von verwendeten Informationssystemen sollten rechtzeitig eingeholt, die Anfälligkeit der Organisation für eine Ausnutzung solcher Schwachstellen sollte bewertet und angemessene Maßnahmen für den Umgang mit dem damit einhergehenden Risiko sollten ergriffen werden.

Umsetzungshinweise

Eine aktuelle und vollständige Aufstellung der Werte (siehe 8) ist eine Vorbedingung für ein wirksames technisches Schwachstellenmanagement. Zu den spezifischen Informationen, die zur Unterstützung des technischen Schwachstellenmanagements benötigt werden, gehören Software-Anbieter, Versionsnummern, der aktuelle Verteilungsstand (z. B. die Angabe, welche Software auf welchen Systemen installiert ist) und die für die Software innerhalb der Organisation zuständige(n) Person(en).

Als Reaktion auf die Feststellung potenzieller technischer Schwachstellen sollten zeitnah entsprechende Abhilfemaßnahmen ergriffen werden. Zur Einrichtung eines effektiven Managementprozesses in Bezug auf technische Schwachstellen sollte die folgende Anleitung beachtet werden:

a) Die Organisation sollte die mit dem technischen Schwachstellenmanagement verbundenen Aufgaben und Zuständigkeiten festlegen und einrichten, die die Überwachung auf Schwachstellen, die Risikobeurteilung von Schwachstellen, das Einspielen von Patches, die Nachverfolgung von Assets und sämtliche erforderlichen Koordinationsaufgaben umfassen;

b) Informationsressourcen, die zur Feststellung relevanter technischer Schwachstellen und deren nachhaltiger Bewusstmachung verwendet werden, sollten hinsichtlich Software und anderer Technologien identifiziert werden (auf Grundlage der Inventarliste der Werte, siehe 8.1.1). Diese Informationsressourcen sollten bei Änderungen im Inventar oder bei Ermittlung neuer oder weiterer nützlicher Ressourcen aktualisiert werden;

c) Es sollte ein Zeitplan zur Reaktion auf Benachrichtigungen über möglicherweise relevante technische Schwachstellen festgelegt werden;

d) Bei Feststellung einer potenziellen technischen Schwachstelle sollte die Organisation die damit verbundenen Risiken feststellen und die erforderlichen Abhilfemaßnahmen bestimmen. Zu diesen können das Patchen der anfälligen Systeme oder die Anwendung anderer Kontrollmaßnahmen gehören;

e) Je nach Dringlichkeit der Behebung einer technischen Schwachstelle sollte die entsprechende Maßnahme nach den für das Änderungsmanagement geltenden Sicherheitsmaßnahmen (siehe 12.1.2) oder anhand der folgenden Abhilfemaßnahmen bei Informationssicherheitsvorfällen (siehe 16.1.5) durchgeführt werden;

f) Wenn ein Patch aus einer vertrauenswürdigen Quelle zur Verfügung steht, sollten die mit der Installation des Patches verbundenen Risiken beurteilt werden (die Risiken durch die Schwachstelle sollten gegenüber den Risiken durch die Installation des Patches abgewogen werden);

g) Die Patches sollten vor der Installation getestet und beurteilt werden, um sicherzustellen, dass sie die gewünschte Wirkung entfalten und zu keinen nicht hinnehmbaren Nebeneffekten führen. Steht kein Patch zur Verfügung, sollten andere Sicherheitsmaßnahmen in Betracht gezogen werden, z. B.:

   1) Abschaltung der Dienste bzw. Funktionen, die von der Schwachstelle betroffen sind;

   2) Anpassung bzw. Ergänzung der Zugriffskontrollen, z. B. Firewalls, an den Netzwerkgrenzen (siehe 13.1);

   3) verstärkte Überwachung zur Erkennung stattfindender Angriffe;

   4) Sensibilisierung der Mitarbeiter für die Schwachstelle.

h) Alle durchgeführten Verfahren sollten in einem Audit-Protokoll vermerkt werden;

i) Der Prozess zum technischen Schwachstellenmanagement sollte regelmäßigüberwacht und bewertet werden, um seine Wirksamkeit und Effizienz sicherzustellen;

j) Hochrisikosysteme sollten bevorzugt behandelt werden;

k) Ein wirkungsvoller Prozess zum technischen Schwachstellenmanagement sollte mit den Aktivitäten zum Umgang mit Sicherheitsvorfällen abgestimmt werden, damit Daten über Schwachstellen an die für Abhilfemaßnahmen zuständige Person weitergeleitet werden und bei einem Sicherheitsvorfall entsprechend durchzuführende technische Verfahren zur Verfügung stehen;

l) Es sollte ein Verfahren zum Umgang mit Situationen festgelegt werden, in denen eine Schwachstelle festgestellt wurde, aber keine geeignete Gegenmaßnahme existiert. In diesen Situationen sollte die Organisation die Risiken beurteilen, die die bekannte Schwachstelle birgt, und geeignete Erkennungs- und Abhilfemaßnahmen festlegen.

Weitere Informationen

Das technische Schwachstellenmanagement kann auch als Unterfunktion des Änderungsmanagements gesehen werden und dabei die Vorteile der Prozesse und Verfahren des Änderungsmanagements nutzen (siehe 12.1.2 und 14.2.2).

Anbieter stehen häufig unter dem erheblichen Druck, Patches so schnell wie möglich zu veröffentlichen. Daher ist es möglich, dass ein Patch das bestehende Problem nicht angemessen behebt und sogar zu negativen Nebeneffekten führt. Zudem ist nach der Anwendung eines Patches dessen Deinstallation nicht ohne weiteres möglich.

Wenn eine angemessene Überprüfung der Patches nicht möglich ist, z. B. aus Kostengründen oder aufgrund fehlender Ressourcen, kann über eine Zurückstellung des Patches nachgedacht werden, um zuvor die damit verbundenen Risiken auf Grundlage der von anderen Benutzern berichteten Erfahrungen abzuschätzen. Die Anwendung von ISO/IEC 27031 kann von Nutzen sein.

12.6.2 Beschränkungen der Software-Installation

Maßnahme

Für Software-Installationen durch Benutzer sollten Regeln festgelegt und implementiert werden.

Umsetzungshinweise

Die Organisation sollte eine strenge Richtlinie in Bezug auf die Art von Software festlegen und umsetzen, die von Anwendern installiert werden darf.

Dabei sollte das „Least Privilege“-Prinzip angewendet werden. Anwendern, denen bestimmte Rechte eingeräumt werden, können Software installieren. Die Organisation sollte festlegen, welche Arten von Softwareinstallationen gestattet sind (z. B. Aktualisierungen und Sicherheitspatches für vorhandene Software) und welche Installationsarten untersagt sind (z. B. Software ausschließlich zur privaten Nutzung sowie Software, von der nicht bekannt ist, ob sie möglicherweise Schadcode enthält oder die in diesem Verdacht steht). Die Gewährung entsprechender Rechte sollte unter Berücksichtigung der Funktionen der jeweiligen Anwender erfolgen.

Weitere Informationen

Durch die unkontrollierte Installation von Software auf Rechnern können Schwachstellen entstehen, die zu einem Informations- oder Integritätsverlust oder anderen Informationssicherheitsvorfällen oder zum Verstoß gegen Rechte an geistigem Eigentum führen.

12.7 Auswirkungen von Audits auf Informationssysteme

Zielsetzung: Minimierung der Auswirkungen von Audit-Aktivitäten auf betriebliche Systeme.

12.7.1 Kontrollen für Audits von Informationssystemen

Maßnahme

Audit-Anforderungen und -Aktivitäten im Zusammenhang mit betriebsrelevanten Systemen sollten sorgfältig geplant und vereinbart werden, um Unterbrechungen der Geschäftsabläufe zu minimieren.

Umsetzungshinweise

Die folgenden Leitlinien sollten beachtet werden:

a) Die Audit-Anforderungen für den Zugriff auf Systeme und Daten sollten mit dem zuständigen Management vereinbart werden;

b) Der Umfang der technischen Audit-Prüfungen sollte vereinbart und kontrolliert werden;

c) Die Audit-Prüfungen sollten auf einen reinen Lesezugriff auf Software und Daten beschränkt sein;

d) Ein über den Lesezugriff hinausgehender Zugang sollte nur in Bezug auf isolierte Kopien von Systemdateien gestattet werden, die nach Abschluss des Audits gelöscht werden oder aber entsprechend geschützt werden sollten, falls eine Verpflichtung besteht, diese Dateien aufgrund geltender Dokumentationsanforderungen bezüglich des Audits aufzubewahren;

e) Es sollten Anforderungen bezüglich einer besonderen oder zusätzlichen Verarbeitung ermittelt und vereinbart werden. Audit-Prüfungen, die Einfluss auf die Systemverfügbarkeit haben könnten, sollten außerhalb der Geschäftszeiten durchgeführt werden;

f) Sämtliche Zugriffe sollten überwacht und protokolliert werden, um auf diese Weise einen Referenz-Prüfpfad zu erstellen.

13 Sicherheit in der Kommunikation

13.1 Netzwerksicherheitsmanagement

Zielsetzung: Sicherstellung des Schutzes von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen.

13.1.1 Netzwerkkontrollen

Maßnahme

Netzwerke sollten so verwaltet und kontrolliert werden, dass die Informationen in Systemen und Anwendungen geschützt sind.

Umsetzungshinweise

Es sollten Maßnahmen umgesetzt werden, um die Sicherheit der Informationen in Netzwerken und den Schutz vernetzter Dienste vor unbefugtem Zugriff zu gewährleisten. Die folgenden Punkte sollten dabei insbesondere berücksichtigt werden:

a) Es sollten Zuständigkeiten und Verfahren für die Verwaltung der Netzwerktechnik festgelegt werden;

b) Die betriebliche Zuständigkeit für die Netzwerke sollte ggf. vom Rechnerbetrieb getrennt werden (siehe 6.1.5);

c) Es sollten besondere Maßnahmen umgesetzt werden, um die Vertraulichkeit und Integrität der über öffentliche Netze oder drahtlose Netzwerke übertragenen Daten zu gewährleisten und um die vernetzten Systeme und Anwendungen zu schützen (siehe 10 und 13.2). Möglicherweise sind auch besondere Maßnahmen erforderlich, um die Verfügbarkeit der Netzwerkdienste und der angeschlossenen Computer aufrechtzuerhalten;

d) Zur Aufzeichnung und Erkennung von Handlungen, die Einfluss auf die Informationssicherheit haben oder für diese relevant sind, sollte eine entsprechende Protokollierung und Überwachung stattfinden;

e) Die Managementaktivitäten sollten genau koordiniert werden, um den Nutzen für die Organisation zu optimieren und um sicherzustellen, dass die Maßnahmen konsistent innerhalb der Datenverarbeitungsinfrastruktur umgesetzt werden;

f) Die Systeme im Netzwerk sollten authentifiziert werden;

g) Die Systemverbindung zum Netzwerk sollte eingeschränkt sein.

Weitere Informationen

Weitere Informationen zur Netzwerksicherheit können ISO/IEC 27033 (Netzwerksicherheit) entnommen werden.

13.1.2 Sicherheit von Netzwerkdiensten

Maßnahme

Es sollten Sicherheitsmechanismen, Service-Level und Anforderungen für die Verwaltung aller Netzwerkdienste ermittelt und in Verträge über Netzwerkdienste aufgenommen werden, und zwar unabhängig davon, ob diese Dienste intern erbracht oder ausgelagert werden.

Umsetzungshinweise

Die Fähigkeit des Bereitstellers von Netzwerkdiensten, die vereinbarten Dienste auf sichere Weise zu erbringen, sollte bestimmt und regelmäßig überwacht werden, und es sollte ein Überprüfungsrecht vereinbart werden.

Die für bestimmte Dienste erforderlichen Sicherheitsvorkehrungen wie Sicherheitsfunktionen, Service-Level und Verwaltungsanforderungen sollten festgestellt werden. Die Organisation sollte sicherstellen, dass die Anbieter von Netzwerkdiensten diese Maßnahmen umsetzen.

Weitere Informationen

Zu den Netzwerkdiensten gehören die Bereitstellung von Verbindungen, Private-Network-Dienste und Mehrwertnetze sowie Managed-Network-Sicherheitslösungen wie Firewalls und Angriffserkennungssysteme. Diese Dienste können von einfachen, unverwalteten Bandbreitendienst- bis zu komplexen Mehrwertdienst-Angeboten reichen.

Bei den Sicherheitsfunktionen des Netzwerkdienste kann es sich handeln um:

a) Technologie, die zur Steigerung der Sicherheit der Netzwerkdienste eingesetzt wird, wie Authentifizierung, Verschlüsselung und Netzwerkverbindungskontrollen;

b) technische Parameter, die für eine abgesicherte Verbindung mit den Netzwerkdiensten entsprechend der Sicherheits- und Netzwerkverbindungsregeln erforderlich sind;

c) Verfahren für die Nutzung der Netzwerkdienste zur ggf. erforderlichen Einschränkung des Zugriffs auf Netzwerkdienste oder Anwendungen.

13.1.3 Trennung in Netzwerken

Maßnahme

Gruppen von Informationsdiensten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Umsetzungshinweise

Eine Methode zum Sicherheitsmanagement in großen Netzwerken besteht in deren Trennung in separate Netzwerkdomänen. Diese Domänen können anhand von Trust-Levels (z. B. Domäne für öffentlichen Zugang, Desktop-Domäne, Server-Domäne), nach Organisationseinheiten (z. B. Personal, Finanzen, Marketing) oder einer Kombination daraus (z. B. Server-Domäne, in der mehrere Organisationseinheiten vernetzt sind) ausgewählt werden. Die Trennung kann mittels physisch unterschiedlicher Netzwerke oder durch Verwendung verschiedener logischer Netzwerke (z. B. Virtual Private Networks) realisiert werden.

Der Bereich jeder einzelnen Domäne sollte genau definiert werden. Der domänenübergreifende Zugang ist gestattet, sollte jedoch mittels eines Gateways (z. B. Firewall, filternder Router) kontrolliert werden. Den Kriterien für die Aufteilung der Netzwerke in Domänen sowie dem über die Gateways gestatteten Zugang sollte eine Beurteilung der Sicherheitsanforderungen der einzelnen Domänen zugrunde liegen. Diese Beurteilung sollte nach der Zugriffskontrollleitlinie (siehe 9.1.1), den Zugangsanforderungen, dem Wert und der Klassifizierung der verarbeiteten Informationen erfolgen, wobei auch die relativen Kosten und die Auswirkungen auf die Leistungsfähigkeit angesichts der Einbeziehung einer geeigneten Gateway-Technologie in Betracht gezogen werden sollten.

Drahtlos-Netzwerke erfordern eine besondere Behandlung aufgrund des ungenau definierten Netzwerkperimeters. In sensiblen Umgebungen sollte darauf geachtet werden, alle Drahtloszugriffe wie externe Verbindungen (siehe 9.4.2) zu behandeln und diesen Zugriff von den internen Netzwerken zu trennen, bis das Gateway entsprechend der Netzwerkkontrollleitlinie (siehe 13.1.1) passiert wurde, um erst dann den Zugriff auf die internen Systeme zu gewähren.

Bei ordnungsgemäßer Implementierung können die Kontrolltechnologien moderner, standardisierter Drahtlosnetzwerke zur Authentifizierung und Verschlüsselung sowie zum Netzwerkzugang auf Benutzerebene für die Direktverbindung zum internen Netzwerk der Organisation ausreichend sein.

Weitere Informationen

Netzwerke erstrecken sich häufig über die Grenzen von Organisationen hinaus, da geschäftliche Partnerschaften geschlossen werden, die die Verbindung oder gemeinsame Nutzung von informationsverarbeitenden und Netzwerk-Einrichtungen erforderlich machen. Durch diese Erweiterungen kann sich das Risiko eines nicht autorisierten Zugangs zu den an das Netzwerk angeschlossenen Informationssystemen einer Organisation erhöhen, die zum Teil sensible oder geschäftskritische Daten enthalten und deshalb vor anderen Netzwerknutzern geschützt werden müssen.

13.2 Informationsübertragung

Zielsetzung: Wahrung der Sicherheit von Informationen, die innerhalb einer Organisation oder im Austausch mit einer externen Stelle übertragen werden.

13.2.1 Leitlinien und Verfahren für die Informationsübertragung

Maßnahme

Es sollten formelle Leitlinien, Verfahren und Kontrollmaßnahmen in Kraft sein, mit denen die Informationsübertragung über alle Arten von Kommunikationseinrichtungen geschützt wird.

Umsetzungshinweise

Im Rahmen der bei der Nutzung von Kommunikationseinrichtungen für die Informationsübertragung zu beachtenden Verfahren und Kontrollmaßnahmen sollten die folgenden Punkte berücksichtigt werden:

a) Entwicklung von Verfahren, um zu verhindern, dass übertragene Informationen abgefangen, kopiert, verändert, umgeleitet oder zerstört werden;

b) Verfahren zur Erkennung von und zum Schutz vor Malware, die durch die Verwendung elektronischer Kommunikationseinrichtungen übertragen werden (siehe 12.2.1);

c) Verfahren zum Schutz übertragener sensibler elektronischer Informationen, die in Form eines Anhangs vorliegen;

d) Richtlinie oder Leitlinien, in denen die zulässige Verwendung der Kommunikationseinrichtungen beschrieben wird (siehe 8.1.3);

e) Verantwortung der Mitarbeiter, externer Parteien und jedweder anderer Benutzer, die Organisation nicht durch z. B. Diffamierung, Mobbing, betrügerisches Auftreten, Weiterleitung von Kettenbriefen, nicht autorisierten Einkauf und ähnliche Handlungen zu kompromittieren;

f) Verwendung von Verschlüsselungstechnologien, z. B. zum Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen (siehe 10);

g) Leitlinien zur Aufbewahrung und Entsorgung sämtlicher Geschäftskorrespondenz, einschließlich Nachrichten, entsprechend der geltenden nationalen und internationalen Gesetze und Vorschriften;

h) Kontrollmaßnahmen und Beschränkungen in Verbindung mit der Nutzung von Kommunikations-einrichtungen, z. B. automatische Weiterleitung von E-Mails an externe E-Mail-Adressen;

i) Anweisung an die Mitarbeiter, entsprechende Vorsichtsmaßnahmen zu treffen, um die Offenlegung vertraulicher Informationen zu verhindern;

j) kein Hinterlassen von vertrauliche Informationen enthaltenden Mitteilungen auf Anrufbeantwortern, da diese beim Wählen einer falschen Nummer von nicht autorisierten Personen wiedergegeben oder möglicherweise auf öffentlichen Systemen bzw. nicht ordnungsnach gespeichert werden;

k) Mitarbeiteranweisung bezüglich der Probleme bei der Nutzung von Faxgeräten oder -diensten, nämlich:

   1) nicht autorisierter Zugriff auf eingebaute Nachrichtenspeicher zum Abruf von Nachrichten;

   2) vorsätzliche oder unbeabsichtigte Programmierung der Maschinen, so dass diese Nachrichten an bestimmte Nummern senden;

   3) Versand von Dokumenten und Nachrichten an eine falsche Nummer durch Verwählen oder Verwendung einer falsch gespeicherten Nummer.

Außerdem sollten die Mitarbeiter ermahnt werden, keine vertraulichen Gespräche in der Öffentlichkeit oder über unsichere Kommunikationskanäle, in offenen Büros und an Versammlungsorten zu führen.

Die Informationsübertragungsdienste sollten allen anzuwendenden gesetzlichen Vorschriften (siehe 18.1) entsprechen.

Weitere Informationen

Die Informationsübertragung kann durch Verwendung einer Anzahl verschiedener Arten von Kommunikationseinrichtungen erfolgen, darunter E-Mail, Telefon, Fax und Videoübertragung.

Der Software-Übertragung kann über verschiedene Wege erfolgen, unter anderem durch Herunterladen aus dem Internet und durch Kauf von Standardprodukten entsprechender Anbieter.

Die geschäftlichen, rechtlichen und sicherheitsbezogenen Implikationen im Zusammenhang mit dem Austausch elektronischer Daten, dem elektronischen Geschäftsverkehr und elektronischen Kommunikationseinrichtungen sowie die Anforderungen für Kontrollmaßnahmen sollten berücksichtigt werden.

13.2.2 Vereinbarungen zum Informationstransfer

Maßnahme

Es sollten Vereinbarungen bezüglich des sicheren Transfers von geschäftlichen Informationen zwischen der Organisation und externen Parteien getroffen werden.

Umsetzungshinweise

Die Vereinbarungen zum Informationstransfer sollten die folgenden Punkte beinhalten:

a) Managementverantwortlichkeiten zur Kontrolle von und zur Mitteilung bezüglich Übertragung, Versand und Empfang;

b) Verfahren zur Sicherstellung der Nachverfolgbarkeit und Unabstreitbarkeit;

c) technische Mindeststandards für Verpackung und Übertragung;

d) Hinterlegungsvereinbarungen;

e) Standards zur Identifizierung des Kurierunternehmens;

f) Verantwortlichkeiten und Haftung bei Informationssicherheitsvorfällen wie Datenverlust;

g) Verwendung eines vereinbarten Kennzeichnungssystems für sensible oder betriebswichtige Informationen, wobei sicherzustellen ist, dass die Kennzeichnungen ohne weiteres verständlich und die Informationen angemessen geschützt sind (siehe 8.2);

h) technische Normen zum Aufzeichnen und Lesen von Informationen und Software;

i) jedwede besonderen Maßnahmen wie Kryptographie, die zum Schutz sensibler Daten erforderlich sind (siehe 10);

j) Einhaltung einer Kontrollkette für Informationen, die transferiert werden;

k) zulässige Zugriffskontrollstufen.

Es sollten Leitlinien, Verfahren und Normen zum Schutz der ausgetauschten Informationen und physischen Medien eingerichtet und angewendet werden (siehe 8.3.3), auf die in den Vereinbarungen zum Informationstransfer hingewiesen wird.

In den die Informationssicherheit betreffenden Inhalten der Vereinbarungen sollte die Sensibilität der betreffenden geschäftlichen Informationen zum Ausdruck kommen.

Weitere Informationen

Die Vereinbarungen können in elektronischer oder Papierform vorliegen und in Form offizieller Verträge ausgeführt sein. Bei vertraulichen Informationen sollten die für deren Transfer verwendeten spezifischen Mechanismen für alle Organisationen und Vereinbarungsformen gleich sein.

13.2.3 Elektronische Nachrichtenübermittlung

Maßnahme

Informationen in elektronischen Nachrichten sollten angemessen geschützt werden.

Umsetzungshinweise

Überlegungen zur Informationssicherheit bei der elektronischen Nachrichtenübermittlung sollten die folgenden Punkte beinhalten:

a) Maßnahmen zum Schutz der Nachrichten vor nicht autorisiertem Zugriff, vor Veränderung oder Denial of Service, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen;

b) Sicherstellung der korrekten Adressierung und Beförderung der Nachricht;

c) Zuverlässigkeit und Verfügbarkeit des Dienstes;

d) rechtliche Überlegungen, zum Beispiel Anforderungen bezüglich elektronischer Signaturen;

e) Einholung einer Genehmigung vor der Nutzung externer öffentlicher Dienste wie Instant Messaging, soziale Netzwerke oder Filesharing;

f) stärkere Authentifizierungsstufen zur Kontrolle des Zugriffs auf öffentlich zugängliche Netze.

Weitere Informationen

Es gibt viele Arten elektronischer Nachrichtenübermittlung wie E-Mail, elektronischer Datenaustausch und soziale Netzwerke, die eine Rolle in der geschäftlichen Kommunikation spielen.

13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Maßnahme

Entsprechend den Bedürfnissen der Organisation in Bezug auf den Schutz von Informationen sollten Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen ermittelt, regelmäßig geprüft und dokumentiert werden.

Umsetzungshinweise

In den Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollte unter Verwendung rechtsverbindlicher Begriffe auf die Anforderungen zum Schutz vertraulicher Informationen eingegangen werden. Die Vertraulichkeits- oder Geheimhaltungsvereinbarungen müssen auf externe Parteien oder Mitarbeiter der Organisation anwendbar sein. Ihre Bestandteile sollten unter Berücksichtigung des Typs der anderen Partei und des dieser gestatteten Zugriffs oder des Umgangs mit den vertraulichen Informationen ausgewählt bzw. hinzugefügt werden. Zur Feststellung der Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollten die folgenden Elemente in Betracht gezogen werden:

a) Definition der zu schützenden Informationen (z. B. vertrauliche Informationen);

b) voraussichtliche Dauer einer Vereinbarung, einschließlich von Fällen, in denen die Vertraulichkeit nicht befristet ist;

c) erforderliche Maßnahmen bei Beendigung einer Vereinbarung;

d) Pflichten und Maßnahmen der Unterzeichner zur Vermeidung einer nicht autorisierten Offenlegung von Informationen;

e) Eigentümerschaft an Informationen, Geschäftsgeheimnissen und geistigem Eigentum und Zusammenhang mit dem Schutz der vertraulichen Informationen;

f) gestattete Nutzung vertraulicher Informationen und Rechte des Unterzeichnenden zur Nutzung der Informationen;

g) Recht zur Überprüfung und Überwachung von Aktivitäten, die vertrauliche Informationen berühren;

h) Verfahren zur Benachrichtigung und Berichterstattung über nicht autorisierte Offenlegung oder Verlust vertraulicher Informationen;

i) Bestimmungen bezüglich Informationen, die bei Auslaufen der Vereinbarung zurückzugeben bzw. zu vernichten sind;

j) Maßnahmen, die bei einem Verstoß gegen die Vereinbarung durchgeführt werden sollen.

Abhängig von den Informationssicherheitsanforderungen einer Organisation muss die Vertraulichkeits- oder Geheimhaltungsvereinbarung möglicherweise um weitere Punkte ergänzt werden.

Die Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollten allen geltenden Gesetzen und Vorschriften der jeweiligen Rechtsordnung entsprechen (siehe 18.1).

Die Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollten regelmäßig sowie bei sie betreffenden Veränderungen überprüft werden.

Weitere Informationen

Vertraulichkeits- oder Geheimhaltungsvereinbarungen sorgen dafür, dass die Daten einer Organisation geschützt sind und die Unterzeichnenden über ihre Pflichten bezüglich des Schutzes, der Nutzung und der verantwortungsvollen und ihren Befugnissen entsprechenden Offenlegung von Informationen unterrichtet werden.

Möglicherweise muss eine Organisation umständeabhängig verschiedene Formen von Vertraulichkeits- oder Geheimhaltungsvereinbarungen treffen.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen für Informationssysteme

Zielsetzung: Gewährleistung, dass Informationssicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Dies schließt die Anforderungen für Informationssysteme ein, die Dienste über öffentliche Netze bereitstellen.

14.1.1 Analyse und Spezifikation von Sicherheitsanforderungen

Maßnahme

Die die Informationssicherheit betreffenden Anforderungen sollten in die Anforderungen für neue Informationssysteme oder Verbesserungen bei bestehenden Informationssystemen aufgenommen werden.

Umsetzungshinweise

Die Anforderungen an die Informationssicherheit sollten mittels verschiedener Methoden wie der Ableitung von zu beachtenden Anforderungen aus Leitlinien und Vorschriften, der Simulation von Bedrohungsszenarien, der Untersuchung von Vorfällen oder der Verwendung von Schwachstellen-Schwellwerten festgestellt werden. Die Ergebnisse dieser Feststellungen sollten dokumentiert und von allen Stakeholdern geprüft werden.

In den Anforderungen und Maßnahmen hinsichtlich der Informationssicherheit sollten der geschäftliche Wert der betreffenden Informationen (siehe 8.2) sowie die potenziellen negativen geschäftlichen Auswirkungen bei einem Fehlen angemessener Sicherheitsmaßnahmen zum Ausdruck kommen.

Feststellung und Verwaltung der Informationssicherheitsanforderungen und der zugehörigen Prozesse sollten in frühen Stadien von Informationssystemprojekten integriert werden. Eine frühzeitige Berücksichtigung von Informationssicherheitsanforderungen, z. B. bereits in der Entwicklungsphase, kann zu wirksameren und kostengünstigen Leistungen beitragen.

Bei den Anforderungen an die Informationssicherheit sollten außerdem die folgenden Punkte berücksichtigt werden:

a) das erforderliche Vertrauensniveau in Bezug auf die vom Benutzer angegebenen Identität zur Ableitung der Anforderungen hinsichtlich der Benutzerauthentifizierung;

b) die Prozesse zur Zugangsbereitstellung und -genehmigung für geschäftliche Nutzer als auch für Nutzer mit Sonderrechten und technische Nutzer;

c) die Informierung von Benutzern und Betreibern über ihre Pflichten und Zuständigkeiten;

d) die erforderlichen Schutzmaßnahmen für die betroffenen Werte, insbesondere in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität;

e) die aus den Geschäftsabläufen abgeleiteten Anforderungen wie die Protokollierung und Überwachung von Transaktionen sowie Anforderungen bezüglich der Unabstreitbarkeit;

f) die Anforderungen, die durch andere Sicherheitsmaßnahmen gegeben sind, z. B. Schnittstellen zu Protokollierungs- und Überwachungssystemen oder Systemen zur Erkennung von Datenverlusten.

Bei Anwendungen, die Dienste über öffentliche Netze bereitstellen oder Transaktionen implementieren, sollten die entsprechenden Maßnahmen in 14.1.2 und 14.1.3 in Betracht gezogen werden.

Wenn Produkte angeschafft werden, sollte ein formeller Prüf- und Erwerbungsprozess eingehalten werden. Die Verträge mit dem Lieferanten sollten den festgestellten Sicherheitsanforderungen Rechnung tragen. Erfüllen die Sicherheitsfunktionen eines vorgeschlagenen Produkts nicht die spezifizierten Anforderungen, sollten vor der Anschaffung das dadurch entstehende Risiko und entsprechende Maßnahmen erörtert werden.

Die zur Verfügung stehende Leitlinie zur Sicherheitskonfiguration des auf die endgültige Software / den Service-Stack des Systems abgestimmten Produkts sollte ausgewertet und implementiert werden.

Es sollten Kriterien für die Zulassung von Produkten festgelegt werden, z. B. in Bezug auf ihre Funktionen, durch die gewährleistet ist, dass die festgestellten Sicherheitsanforderungen erfüllt werden. Die Produkte sollten vor dem Kauf anhand dieser Kriterien bewertet werden. Zusätzliche Funktionen sollte geprüft werden, um sicherzustellen, dass durch sie keine inakzeptablen, zusätzlichen Risiken entstehen.

Weitere Informationen

ISO/IEC 27005 und ISO 31000 enthalten Leitlinien zur Anwendung von Risikomanagement-Prozessen für die Ermittlung von Sicherheitsmaßnahmen zur Einhaltung der Informationssicherheitsanforderungen.

14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzen

Maßnahme

Informationen im Zusammenhang mit Anwendungsdiensten, die über öffentliche Netze übertragen werden, sollten gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, nicht autorisierte Offenlegung oder Veränderung geschützt werden.

Umsetzungshinweise

Bei den Überlegungen zur Informationssicherheit im Zusammenhang mit Anwendungsdiensten, die über öffentliche Netze übertragen werden, sollten die folgenden Punkte berücksichtigt werden:

a) das Vertrauensniveau, das für eine Partei in Bezug auf die von einer anderen Partei angegebenen Identität erforderlich ist, z. B. durch Authentifizierung;

b) Genehmigungsprozesse im Zusammenhang mit der Frage, wer die Inhalte wichtiger Transaktionsdokumente genehmigen, diese herausgeben oder unterzeichnen darf;

c) Sicherstellung, dass die Kommunikationspartner vollständig über ihre Befugnisse zur Bereitstellung oder Nutzung des Dienstes informiert sind;

d) Bestimmung und Erfüllung von Anforderungen in Bezug auf Vertraulichkeit, Integrität, den Nachweis des Versands und Erhalts wichtiger Dokumente und die Unabstreitbarkeit von Verträgen, z. B. in Verbindung mit Angebots- und Vertragsprozessen;

e) das erforderliche Vertrauen in die Integrität wichtiger Dokumente;

f) die Schutzanforderungen für vertrauliche Informationen;

g) die Vertraulichkeit und Integrität jedweder Auftragstransaktionen, Zahlungsinformationen, Lieferadressen-Details und Empfangsbestätigungen;

h) der angemessene Aufwand zur Verifizierung der von einem Kunden angegebenen Zahlungsinformationen;

i) Auswahl der am besten zur Betrugsvorbeugung geeigneten Zahlungsabwicklungsform;

j) der erforderliche Schutzstufe zur Gewährleistung der Vertraulichkeit und Integrität der Auftragsdaten;

k) Verhinderung von Verlust oder Vervielfältigung der Transaktionsinformationen;

l) Haftung in Bezug auf betrügerische Transaktionen;

m) Versicherungsanforderungen.

Auf viele der oben genannten Punkte kann durch die Anwendung von kryptographischen Maßnahmen (siehe 10) unter Berücksichtigung der Einhaltung der gesetzlichen Vorschriften eingegangen werden (siehe 18, siehe insbesondere 18.1.5 zur Gesetzgebung zum Thema Kryptographie).

Regelungen zwischen Partnern im Zusammenhang mit Anwendungsdiensten sollte eine dokumentierte Vereinbarung zugrunde liegen, die beide Parteien zur Einhaltung der vereinbarten Dienstbedingungen einschließlich der Genehmigungsdetails verpflichtet (siehe b) oben).

Es sollten Anforderungen bezüglich der Widerstandsfähigkeit gegen Angriffe berücksichtigt werden. Dazu können Anforderungen zum Schutz der betreffenden Anwendungsserver oder zur Sicherstellung der Verfügbarkeit zur Bereitstellung des Dienstes erforderlicher Netzkupplungen gehören.

Weitere Informationen

Anwendungen, auf die über öffentliche Netze zugegriffen werden kann, sind einer Reihe netzbezogener Bedrohungen durch betrügerische Aktivitäten, Vertragsstreitigkeiten oder unrechtmäßige Veröffentlichung von Informationen ausgesetzt. Daher sind eine ausführliche Risikoeinschätzung und eine sorgfältige Auswahl von Kontrollmaßnahmen unverzichtbar. Zu den erforderlichen Kontrollmaßnahmen gehören häufig Verschlüsselungsverfahren für die Authentifizierung und die sichere Datenübertragung.

Anwendungsdienste können sich sicherer Authentifizierungsverfahren wie einer Public-Key-Verschlüsselung und digitaler Signaturen bedienen (siehe 10), um die Risiken zu verringern. Außerdem kann auf Trusted Third Parties (TTPs) zurückgegriffen werden, wenn diese Dienste benötigt werden.

14.1.3 Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten

Maßnahme

Informationen, die im Zuge von Transaktionen im Zusammenhang mit Anwendungsdiensten übertragen werden, sollten geschützt werden, um unvollständigen Übertragungen und Fehlleitungen sowie nicht autorisierten Offenlegungen, Vervielfältigungen oder wiederholten Wiedergaben von Nachrichten vorzubeugen.

Umsetzungshinweise

Überlegungen zur Informationssicherheit bei Transaktionen im Zusammenhang mit Anwendungsdiensten sollten die folgenden Punkte beinhalten:

a) Nutzung elektronischer Signaturen durch alle an der Transaktion beteiligten Personen;

b) sämtliche Aspekte der Transaktion, also Sicherstellung, dass:

   1) die geheimen Benutzerauthentifizierungsinformationen bei allen Parteien gültig und verifiziert sind;

   2) die Transaktion vertraulich bleibt;

   3) die Privatsphäre aller beteiligten Parteien gewährleistet wird;

c) verschlüsselter Kommunikationsweg zwischen allen beteiligten Parteien;

d) Sicherung der zur Kommunikation zwischen allen beteiligten Parteien verwendeten Protokolle;

e) Sicherstellung, dass die Speicherung der Transaktionsdaten an einem nicht öffentlich zugänglichen Ort erfolgt, z. B. einer Storage-Plattform im Intranet der Organisation, und nicht auf einem Speichermedium aufbewahrt und zur Verfügung gestellt wird, das direkt über das Internet zugänglich ist;

f) bei Verwendung einer Zertifizierungsstelle (z. B. zur Ausgabe und Unterhaltung digitaler Signaturen oder digitaler Zertifikate): Integration und Einbettung der Sicherheit über den gesamten End-to-End-Zertifikats-/Signatur-Management-Prozess.

Weitere Informationen

Der Umfang der verwendeten Kontrollmaßnahmen muss dem Risikoniveau der einzelnen, mit den Anwendungsdiensten in Zusammenhang stehenden Transaktionsformen entsprechen.

Die Transaktionen müssen möglicherweise bestimmten gesetzlichen und behördlichen Anforderungen der Rechtsordnung entsprechen, in der die Transaktion erzeugt, verarbeitet, abgeschlossen oder gespeichert wurde.

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Zielsetzung: Sicherstellung, dass Informationssicherheit im Rahmen des Entwicklungszyklus von Informationssystemen konzipiert und implementiert wird.

14.2.1 Leitlinie für sichere Entwicklung

Maßnahme

Es sollten Regeln für die Entwicklung von Software und Systemen festgelegt und bei Entwicklungen innerhalb der Organisation angewandt werden.

Umsetzungshinweise

Die sichere Entwicklung eine Anforderungen zum Aufbau eines sicheren Dienstes, einer sicheren Architektur und Software und eines sicheren Systems. Im Rahmen einer Leitlinie zur sicheren Entwicklung sollten die folgenden Aspekte in Betracht gezogen werden:

a) Sicherheit der Entwicklungsumgebung;

b) Leitlinie bezüglich der Sicherheit im Softwareentwicklungsprozess;

   1) Sicherheit in der Softwareentwicklungsmethodik;

   2) Leitlinien zur sicheren Programmierung für jede verwendete Programmiersprache;

c) Sicherheitsanforderungen in der Entwurfsphase;

d) Sicherheitsüberprüfungen innerhalb der Projektmeilensteine;

e) sichere Repositories;

f) Sicherheit bei der Versionskontrolle;

g) erforderliches Wissen um die Anwendungssicherheit;

h) Fähigkeit der Entwickler, Schwachstellen zu vermeiden, zu finden und zu beheben.

Sichere Programmiertechniken sollten sowohl bei Neuentwicklungen als auch bei der Wiederverwendung vorhandenen Codes verwendet werden, bei dem die bei der Entwicklung angewendeten Standards möglicherweise nicht bekannt sind oder nicht den aktuellen Best Practices entsprechen. Sichere Programmierstandards sollten berücksichtigt und dort, wo dies relevant ist, verpflichtend gemacht werden. Die Entwickler sollten in deren Verwendung geschult werden, und die Verwendung sollte mit Hilfe von Tests und Code-Prüfungen verifiziert werden.

Wenn die Entwicklung ausgelagert wird, sollte die Organisation die Zusicherung verlangen, dass die externe Partei diese Regeln für sichere Entwicklung einhält (siehe 14.2.7).

Weitere Informationen

Die Entwicklung kann auch innerhalb von Anwendungen stattfinden (Büroanwendungen, Scripting, Browser und Datenbanken).

14.2.2 Änderungskontrollverfahren

Maßnahme

Änderungen an Systemen innerhalb des Entwicklungszyklus sollten durch die Anwendung formeller Änderungskontrollverfahren kontrolliert werden.

Umsetzungshinweise

Es sollten formelle Änderungskontrollverfahren dokumentiert und umgesetzt werden, um die Integrität des Systems, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen. Die Einführung neuer Systeme und wesentlicher Änderungen an den bestehenden Systemen sollte nach einem formellen Prozess erfolgen, der Dokumentation, Spezifikation, Prüfung, Qualitätskontrolle und begleitete Umsetzung umfasst.

Dieser Prozess sollte eine Risikoeinschätzung, eine Analyse der Auswirkungen durch die Änderungen und die Spezifikation der erforderlichen Sicherheitskontrollen umfassen. Im Rahmen dieses Prozesses sollte außerdem sichergestellt werden, dass bestehende Sicherheits- und Kontrollverfahren nicht beeinträchtigt werden, dass den Support-Programmierern nur der Zugriff auf Teile des Systems gewährt wird, die sie für ihre Arbeit benötigen und dass für jede Änderung eine offizielle Zustimmung und Genehmigung eingeholt wird.

Kontrollverfahren für betriebliche und Anwendungsänderungen sollten möglichst integriert werden (siehe 12.1.2). In den Änderungskontrollverfahren sollten unter anderem die folgenden Punkte berücksichtigt werden:

a) Führen eines Verzeichnisses vereinbarter Berechtigungsebenen;

b) Sicherstellung, dass Änderungen nur von autorisierten Benutzern übermittelt werden;

c) Überprüfung der Kontrollmaßnahmen und Integritätsverfahren, um sicherzustellen, dass sie nicht von den Änderungen beeinträchtigt werden;

d) Ermittlung sämtlicher Software, Informationen, Datenbankeinträge und Hardware, die einer Ergänzung bedarf bzw. bedürfen;

e) Feststellung und Überprüfung sicherheitskritischen Codes, um die Wahrscheinlichkeit bekannter Sicherheitsschwachstellen möglichst gering zu halten;

f) Einholung einer offiziellen Genehmigung für detaillierte Vorschläge vor Arbeitsbeginn;

g) Sicherstellung, dass entsprechend autorisierte Benutzer den Änderungen vor der Umsetzung zustimmen;

h) Sicherstellung, dass die Systemdokumentation nach Abschluss jeder Änderung aktualisiert und die alte Dokumentation archiviert oder entsorgt wird;

i) Durchführung einer Versionskontrolle bei allen Software-Aktualisierungen;

j) Pflege eines Prüfpfads aller Änderungsanforderungen;

k) Sicherstellung, dass die Betriebsdokumentation (siehe 12.1.1) und die Benutzerverfahren nach Bedarf entsprechend geändert werden;

l) Sicherstellung, dass die Umsetzung von Änderungen rechtzeitig erfolgt und die betreffenden Geschäftsprozesse dadurch nicht gestört werden.

Weitere Informationen

Software-Änderungen können Einfluss auf die Betriebsumgebung haben und umgekehrt.

Es empfiehlt sich, die Überprüfung neuer Software in einer Umgebung durchzuführen, die sowohl von der Produktions- als auch von der Entwicklungsumgebung getrennt ist (siehe 12.1.4). Dadurch bietet sich ein Kontrollinstrument für neue Software, und ein zusätzlicher Schutz der Betriebsinformationen, die für Prüfzwecke verwendet werden, wird ermöglicht. Dies gilt für Patches, Service Packs und andere Aktualisierungen.

Sofern automatische Aktualisierungen in Betracht gezogen werden, sollte das Risiko für die Integrität und Verfügbarkeit des Systems gegenüber dem Vorteil einer möglichst schnellen Einspielung von Aktualisierungen abgewogen werden. Automatische Aktualisierungen sollten nicht bei kritischen Systemen angewendet werden, da manche Aktualisierungen zum Ausfall kritischer Anwendungen führen können.

14.2.3 Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform

Maßnahme

Bei einem Wechsel der Betriebsplattform sollten geschäftskritische Anwendungen geprüft und getestet werden, um sicherzustellen, dass es zu keinen negativen Auswirkungen auf die Betriebstätigkeit oder die Sicherheit der Organisation kommt.

Umsetzungshinweise

Dieser Prozess sollte folgende Punkte umfassen:

a) Überprüfung der Verfahren zur Anwendungskontrolle und Integritätsgewährleistung, um sicherzustellen, dass diese von den Änderungen der Betriebsplattform nicht beeinträchtigt werden;

b) Sicherstellung, dass eine rechtzeitige Benachrichtigung über Änderungen der Betriebsplattform erfolgt, um die Durchführung entsprechender Tests und Überprüfungen vor der Umsetzung zu ermöglichen;

c) Sicherstellung, dass entsprechende Änderungen an den Geschäftskontinuitätsplänen vorgenommen werden (siehe 17).

Weitere Informationen

Zu den Betriebsplattformen zählen Betriebssysteme, Datenbanken und Middleware-Plattformen. Die Kontrollmaßnahmen sollten auch bei Anwendungsänderungen angewendet werden.

14.2.4 Beschränkung von Änderungen an Software-Paketen

Maßnahme

Von Änderungen an Software-Paketen sollte abgeraten werden. Falls doch Änderungen vorgenommen werden, sollten diese auf das Notwendige beschränkt sein und in jedem Fall streng kontrolliert werden.

Umsetzungshinweise

Die vom Anbieter bereitgestellten Software-Pakete sollten, soweit möglich und praktikabel, ohne Änderungen verwendet werden. Falls jedoch ein Software-Paket verändert werden muss, sollten die folgenden Punkte berücksichtigt werden:

a) das Risiko, dass eingebaute Kontrollmechanismen und Integritätsprozesse beeinträchtigt werden;

b) die möglicherweise erforderliche Einholung der Zustimmung des Anbieters;

c) die Möglichkeit, die erforderlichen Änderungen vom Anbieter in Form einer normalen Programmaktualisierung zu erhalten;

d) die Auswirkungen, falls die Organisation durch die Änderungen künftig die Wartung der Software übernehmen muss;

e) die Kompatibilität mit der anderen verwendeten Software.

Falls Änderungen erforderlich sind, sollten die Originalsoftware aufbewahrt und die Änderungen an einer dafür bestimmten Kopie vorgenommen werden. Es sollte ein Managementprozess für die Software-Aktualisierung implementiert werden, um sicherzustellen, dass die aktuellsten genehmigten Patches und Anwendungs-aktualisierungen für sämtliche autorisierte Software installiert werden (siehe 12.6.1). Sämtliche Änderungen sollten vollständig getestet und dokumentiert werden, so dass sie ggf. bei zukünftigen Software-Upgrades erneut angewendet werden können. Sofern erforderlich, sollten die Änderungen getestet und von einer unabhängigen Prüfstelle validiert werden.

14.2.5 Leitlinien zur sicheren Systementwicklung

Maßnahme

Es sollten Grundsätze für die Entwicklung sicherer Systeme festgelegt, dokumentiert, aufrechterhalten und bei jedem Vorhaben zur Implementierung eines Informationssystems angewendet werden.

Umsetzungshinweise

Für interne Entwicklungsaktivitäten am Informationssystem sollten sichere Entwicklungsverfahren auf Grundlage von Prinzipien des Sicherheitsengineerings eingerichtet, dokumentiert und angewendet werden. Sicherheitsaspekte sollte bei der Entwicklung sämtlicher Architekturschichten (Geschäft, Daten, Anwendungen und Technologie) berücksichtigt werden, wobei zwischen den Anforderungen an Informationssicherheit und Zugänglichkeit abgewogen werden muss. Neue Technologien sollten hinsichtlich ihrer Sicherheitsrisiken analysiert und der Entwurf mit Blick auf bekannte Angriffsmuster überprüft werden.

Diese Prinzipien und die festgelegten Entwicklungsverfahren sollten regelmäßig überprüft werden, um sicherzustellen, dass sie wirksam zu verbesserten Sicherheitsstandards innerhalb des Entwicklungsprozesses beitragen. Außerdem sollten sie regelmäßig überprüft werden, um sicherzustellen, dass sie bezüglich der Abwehr neuer potenzieller Bedrohungen nach wie vor aktuell sind und dass sie an Fortschritte bei Technologien und Lösungen angepasst werden können.

Die festgelegten Prinzipien des Sicherheitsengineerings sollten über die Verträge und anderen verbindlichen Vereinbarungen zwischen der Organisation und dem jeweiligen Outsourcing-Partner ggf. auch auf ausgelagerte Informationssysteme angewendet werden. Die Organisation sollte sich davon überzeugen, dass die Sicherheitsengineering-Prinzipien des Vertragspartners ähnlich streng sind wie die eigenen.

Weitere Informationen

Die Anwendungsentwicklungsverfahren sollten für die Entwicklung von Anwendungen mit Eingabe- und Ausgabeschnittstellen sichere Entwicklungstechniken vorsehen. Sichere Entwicklungstechniken bieten eine Anleitung für Benutzerauthentifizierungstechniken, eine sichere Sitzungssteuerung und Datenvalidierung sowie die Bereinigung und Entfernung von Debug-Code.

14.2.6 Sichere Entwicklungsumgebung

Maßnahme

Organisationen sollten sichere Entwicklungsumgebungen für Systementwicklungen und Integrationsvorhaben, die den gesamten Zyklus der Systementwicklung abdecken, einrichten und angemessen schützen.

Umsetzungshinweise

Eine sichere Entwicklungsumgebung umfasst Personen, Prozesse und Technologien in Verbindung mit der Systementwicklung und -integration.

Die Organisationen sollten die mit den einzelnen Systementwicklungsvorhaben verbundenen Risiken beurteilen und sichere Entwicklungsumgebungen für die spezifischen Systementwicklungsvorhaben einrichten, und zwar unter Berücksichtigung der folgenden Punkte:

a) Sensibilität der vom System zu verarbeitenden, speichernden und übertragenden Daten;

b) bestehende externe und interne Anforderungen, z. B. aufgrund von Vorschriften oder Leitlinien;

c) bereits von der Organisation umgesetzte Sicherheitsmaßnahmen, die die Systementwicklung unterstützen;

d) Vertrauenswürdigkeit der in dieser Umgebung arbeitenden Personen (siehe 7.1.1);

e) Ausmaß der Arbeitsauslagerung im Zusammenhang mit der Systementwicklung;

f) erforderliche Trennung zwischen den Entwicklungsumgebungen;

g) Kontrolle des Zugangs zur Entwicklungsumgebung;

h) Überwachung von Änderungen an der Umgebung und darin gespeichertem Code;

i) Backups werden an sicheren, externen Standorten gespeichert;

j) Kontrolle über den Datenverkehr aus der und in die Umgebung.

Nachdem die Schutzstufe für eine bestimmte Entwicklungsumgebung festgelegt worden ist, sollten die Organisationen die entsprechenden Prozesse im Rahmen sicherer Entwicklungsverfahren dokumentieren und diese allen Personen bereitstellen, die sie benötigen.

14.2.7 Ausgelagerte Entwicklung

Maßnahme

Die Organisation sollte ausgelagerte Systementwicklungstätigkeiten beaufsichtigen und überwachen.

Umsetzungshinweise:

Bei der Auslagerung von Systementwicklungstätigkeiten sollten die folgenden Punkte über die gesamte externe Lieferkette der Organisation berücksichtigt werden:

a) Lizenzierungsmodelle, Eigentümerschaft an Programmcode und geistige Eigentumsrechte in Bezug auf die ausgelagerten Inhalte (siehe 18.1.2);

b) vertragliche Anforderungen bezüglich des sicheren Entwurfs, der Programmierung und der Überprüfungspraxis (siehe 14.2.1);

c) Bereitstellung des genehmigten Bedrohungsmodells für den externen Entwickler;

d) Abnahmeprüfung bezüglich der Qualität und Genauigkeit der bereitgestellten Leistungen;

e) Vorlage von Nachweisen, dass Sicherheitsschwellen verwendet wurden, um zulässige Mindeststandards in Bezug auf Sicherheit und Einhaltung der Privatsphäre festzulegen;

f) Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um zu gewährleisten, dass bei Auslieferung kein vorsätzlich oder versehentlich eingefügter Schadcode enthalten ist;

g) Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um das Vorhandensein bekannter Schwachstellen auszuschließen;

h) Hinterlegungsvereinbarungen, z. B. wenn der Quellcode nicht mehr verfügbar ist;

i) vertragliches Recht zur Überprüfung der Entwicklungsprozesse und Kontrollmaßnahmen;

j) effektive Dokumentation der zur Erzeugung der bereitgestellten Leistungen verwendeten Build-Umgebung;

k) die Organisation ist weiterhin verantwortlich für die Einhaltung der geltenden Gesetze und die Verifizierung der Kontrollwirksamkeit.

Weitere Informationen

Weitere Informationen zu Lieferantenbeziehungen können ISO/IEC 27036 entnommen werden.

14.2.8 Systemsicherheitsprüfungen

Maßnahme

Während der Entwicklung sollte die Funktion der Sicherheitsfunktionen geprüft werden.

Umsetzungshinweise

Neue und aktualisierte Systeme müssen während der Entwicklungsprozesse eine gründliche Überprüfung und Verifizierung erfahren, einschließlich der Vorbereitung einer detaillierten Planung der Aktivitäten, Testeingaben und erwarteten Ausgaben unter verschiedenen Bedingungen. Wie bei internen Entwicklungsvorhaben sollten derartige Prüfungen zunächst vom Entwicklungsteam durchgeführt werden. Danach sollten unabhängige Abnahmeprüfungen unternommen werden (sowohl bei internen als auch bei ausgelagerten Entwicklungsvorhaben), um sicherzustellen, dass das System wie erwartet (und nur wie erwartet) funktioniert (siehe 14.1.1 und 14.1.2). Der Umfang der Prüfungen sollte der Bedeutung und der Beschaffenheit des Systems entsprechen.

14.2.9 Systemabnahmeprüfung

Maßnahme

Für neue Informationssysteme, Upgrades und neue Versionen sollten Abnahmeprüfungsprogramme und dazugehörige Kriterien festgelegt werden.

Umsetzungshinweise

Die Systemabnahmeprüfung sollte die Überprüfung der Informationssicherheitsanforderungen (siehe 14.1.1 und 14.1.2) und der Einhaltung sicherer Systementwicklungspraktiken (siehe 14.2.1) umfassen. Die Überprüfung sollte auch bei erhaltenen Komponenten und integrierten Systemen vorgenommen werden. Die Organisationen können sich automatischer Tools wie Codeanalyse-Tools oder Schwachsteller-Scanner bedienen und sollten sich von der Behebung sicherheitsbezogener Defizite überzeugen.

Die Überprüfung sollte in einer realitätsnahen Testumgebung durchgeführt werden, um sicherzustellen, dass das System keine Schwachstellen in der Betriebsumgebung der Organisation verursacht und dass die Überprüfungen zuverlässig sind.

14.3 Prüfdaten

Zielsetzung: Sicherstellung des Schutzes von zu Prüfzwecken verwendeten Daten.

14.3.1 Schutz von Prüfdaten

Maßnahme

Prüfdaten sollten sorgfältig ausgewählt, geschützt und kontrolliert werden.

Umsetzungshinweise

Die Verwendung von betrieblichen Daten für Prüfzwecke, die personenbezogene Informationen oder andere vertrauliche Informationen enthalten, sollte vermieden werden. Wenn personenbezogene Informationen oder andere vertrauliche Informationen für Prüfzwecke verwendet werden, sollten alle sensiblen Details und Inhalte durch Entfernung oder Veränderung geschützt werden (siehe ISO/IEC 29101).

Die folgenden Leitlinien sollten zum Schutz betrieblicher Daten bei deren Nutzung für Prüfzwecke angewendet werden:

a) Die Zugangskontrollverfahren, die für die betrieblichen Anwendungssysteme gelten, sollten auch für die Prüfanwendungssysteme gelten;

b) Es sollte jedes Mal eine separate Berechtigung erfolgen, wenn Betriebsinformationen in eine Testumgebung kopiert werden;

c) Nach Abschluss der Überprüfung sollten die Betriebsinformationen aus der Testumgebung gelöscht werden;

d) Das Kopieren und die Verwendung von Betriebsinformationen sollte protokolliert werden, so dass ein Prüfpfad existiert.

Weitere Informationen

Die System- und Abnahmeprüfung erfordert meist erhebliche Mengen an Prüfdaten, die den Betriebsdaten möglichst ähnlich sein sollten.

15 Lieferantenbeziehungen

15.1 Informationssicherheit bei Lieferantenbeziehungen

Zielsetzung: Sicherstellung des Schutzes der für Lieferanten zugänglichen Werte des Unternehmens.

15.1.1 Informationssicherheitsleitlinie für Lieferantenbeziehungen

Maßnahme

Anforderungen an die Informationssicherheit zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens sollten mit dem Lieferanten vereinbart und dokumentiert werden.

Umsetzungshinweise

Die Organisationen sollten Maßnahmen zur Informationssicherheit festlegen und anordnen, um spezifisch in Form einer Leitlinie den Zugriff von Lieferanten auf die Informationen der Organisation zu regeln. Diese Maßnahmen sollten auf Prozesse und Verfahren eingehen, die von der Organisation umgesetzt werden müssen, sowie Prozesse und Verfahren, deren Umsetzung durch den Lieferanten die Organisation verlangt. Dazu zählen:

a) Feststellung und Dokumentation der Arten von Lieferanten, z. B. IT-Dienstleistungen, Logistik und Versorgungseinrichtungen, IT-Infrastruktur-Komponenten, mit deren Hilfe die Organisation auf ihre Informationen zugreift;

b) ein standardisierter Prozess und Lebenszyklus zum Management der Lieferantenbeziehungen;

c) Festlegung der jeweiligen Art und Weise der Informationszugriffs für die verschiedenen Arten von Lieferanten sowie Überwachung und Kontrolle des Zugriffs;

d) Mindestanforderungen an die Informationssicherheit für jede Informations- und Zugriffsart als Grundlage für die einzelnen Lieferantenverträge entsprechend den geschäftlichen Bedürfnissen und Anforderungen der Organisation sowie ihrem Risikoprofil;

e) Prozesse und Verfahren zur Überwachung der Einhaltung der festgelegten Anforderungen an die Informationssicherheit für jede Lieferanten- und Zugriffsart, einschließlich Überprüfung durch Dritte und Produktvalidierung;

f) Genauigkeits- und Vollständigkeitskontrollen zur Sicherstellung der Integrität der Informationen bzw. der von den einzelnen Parteien vorgenommenen Informationsverarbeitung;

g) für die Lieferanten geltende Verpflichtungen zum Schutz der Informationen der Organisation;

h) Umgang mit Vorfällen und Gefahren im Zusammenhang mit dem Lieferantenzugriff einschließlich Verantwortlichkeiten sowohl der Organisation als auch der Lieferanten;

i) Vorkehrungen bezüglich Ausfallsicherheit sowie ggf. zur Wiederherstellung und für den Notfall, um die Verfügbarkeit der Informationen bzw. der von den einzelnen Parteien vorgenommenen Informationsverarbeitung sicherzustellen;

j) Sensibilisierungsschulung für die mit Anschaffungen betrauten Mitarbeiter der Organisation bezüglich geltender Leitlinien, Prozesse und Verfahren;

k) Sensibilisierungsschulung für die Mitarbeiter der Organisation, die Umgang mit Mitarbeitern des Lieferanten haben, bezüglich der entsprechenden Beauftragungsrichtlinien und des richtigen Verhaltens je nach Art des Lieferanten und dessen Zugriffsbefugnis auf die Systeme und Informationen der Organisation;

l) Bedingungen, unter denen die Anforderungen an die Informationssicherheit und die entsprechenden Kontrollen in einer von beiden Parteien unterzeichneten Vereinbarung dokumentiert werden;

m) Management der erforderlichen Übergabe von Informationen, informationsverarbeitenden Einrichtungen u. a. und Sicherstellung, dass die Informationssicherheit während der gesamten Übergabephase gewahrt bleibt.

Weitere Informationen

Lieferanten mit einem unzureichenden Informationssicherheitsmanagement können die Vertraulichkeit von Informationen gefährden. Es sollten Kontrollmaßnahmen festgelegt und angewendet werden, um den Lieferantenzugriff auf informationsverarbeitende Einrichtungen zu regeln. So sollten beispielsweise Geheimhaltungsvereinbarungen geschlossen werden, wenn ein besonderes Bedürfnis besteht, die Informationen vertraulich zu halten. Ein weiteres Beispiel sind Datenschutzrisiken, wenn die Lieferantenverträge den Transfer von bzw. den Zugriff auf Informationen über Ländergrenzen hinweg vorsieht. Der Organisation muss stets bewusst sein, dass ihr die rechtliche bzw. vertragliche Verantwortung für den Schutz der Informationen obliegt.

15.1.2 Sicherheitsthemen in Lieferantenverträgen

Maßnahme

Mit jedem Lieferanten, der u. U. auf Informationen der Organisation zugreift, sie verarbeitet, speichert, weitergibt oder IT-Infrastrukturkomponenten dafür bereitstellt, sollten alle relevanten Informationssicherheitsanforderungen festgelegt und vereinbart werden.

Umsetzungshinweise

Lieferantenverträge sollten festgelegt und dokumentiert werden, um sicherzustellen, dass es zu keinen Missverständnissen zwischen der Organisation und dem Lieferanten in Bezug auf die Verpflichtungen der beiden Parteien bezüglich der Erfüllung der relevanten Anforderungen an die Informationssicherheit kommt.

Die folgenden Bestimmungen sollten bei der Abfassung der Vereinbarungen zwecks Erfüllung der Anforderungen an die Informationssicherheit berücksichtigt werden:

a) Beschreibung der Informationen, die bereitgestellt/auf die zugegriffen werden soll und Methoden für die Bereitstellung der/den Zugriff auf die Informationen;

b) Klassifizierung der Informationen nach dem Klassifizierungsschema der Organisation (siehe 8.2), sofern erforderlich auch Abgleich des eigenen Klassifizierungsschemas der Organisation mit jenem des Lieferanten;

c) gesetzliche und behördliche Anforderungen, einschließlich Datenschutz, geistige Eigentumsrechte und Urheberrecht, sowie eine Beschreibung, wie deren Einhaltung sichergestellt wird;

d) Verpflichtung der Vertragsparteien zur Umsetzung einer Reihe vereinbarter Kontrollmaßnahmen, die Zugriffskontrolle, Leistungsüberprüfung, Überwachung, Berichterstattung und Auditing umfassen;

e) Regeln zur zulässigen Nutzung sowie ggf. bezüglich der unzulässigen Nutzung von Informationen;

f) entweder Namensliste von Mitarbeitern des Lieferanten, die befugt sind, auf die Informationen der Organisation zuzugreifen oder diese zu erhalten oder Bedingungen für Mitarbeiter des Lieferanten in Bezug auf Befugniserteilung und -entzug hinsichtlich des Zugriffs auf bzw. des Erhalts von Informationen der Organisation;

g) Leitlinien zur Informationssicherheit, die für den jeweiligen Vertrag relevant sind;

h) Anforderungen und Verfahren für das Vorfallsmanagement (insbesondere Benachrichtigung und Zusammenarbeit bei der Behebung von Vorfällen);

i) Anforderungen bezüglich Schulung und Sensibilisierung für bestimmte Verfahren und Anforderungen an die Informationssicherheit, z. B. für Abhilfemaßnahmen und Autorisierungsverfahren;

j) relevante Vorschriften für Unteraufträge, einschließlich der umzusetzenden Kontrollmaßnahmen;

k) relevante Vertragspartner, einschließlich einer Kontaktperson bei Fragen der Informationssicherheit;

l) ggf. bestehende Überprüfungsanforderungen in Bezug auf die Mitarbeiter des Lieferanten, einschließlich Zuständigkeiten für die Durchführung der Überprüfung und Benachrichtigungsverfahren, falls die Überprüfung nicht vollständig durchgeführt wurde oder das Ergebnis Anlass für Zweifel oder Bedenken gibt;

m) Recht zur Überprüfung der Lieferantenprozesse und Kontrollmaßnahmen im Zusammenhang mit dem Vertrag;

n) Fehlerbehebungs- und Konfliktlösungsprozesse;

o) Verpflichtung des Lieferanten, in regelmäßigen Abständen einen unabhängigen Bericht zur Wirksamkeit der Kontrollmaßnahmen vorzulegen und Zusicherung, relevante Probleme zu beheben, die im Bericht erwähnt werden;

p) Verpflichtungen des Lieferanten, die Sicherheitsanforderungen der Organisation einzuhalten.

Weitere Informationen

Die Verträge verschiedener Organisationen mit verschiedenen Arten von Lieferanten können sich beträchtlich voneinander unterscheiden. Daher sollte sorgfältig darauf geachtet werden, alle relevanten Risiken und Anforderungen in Bezug auf die Informationssicherheit aufzuführen. In Lieferantenverträge können auch weitere Parteien involviert sein (z. B. Unterlieferanten).

Die Verfahren zur Fortsetzung der Verarbeitung für den Fall, dass der Lieferant nicht mehr in der Lage ist, seine Produkte oder Diensten bereitzustellen, müssen im Vertrag berücksichtigt werden, um jedwede Verzögerung bei der Ersatzbeschaffung von Produkten und Diensten zu vermeiden.

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Maßnahme

Vereinbarungen mit Lieferanten sollten Anforderungen für den Umgang mit Informationssicherheitsrisiken im Zusammenhang mit der Dienst- und Produktlieferkette im Bereich der Informations- und Kommunikationstechnologie enthalten.

Umsetzungshinweise

Die folgenden Themen sollten in den Lieferantenverträgen im Zusammenhang mit der Sicherheit der Lieferkette berücksichtigt werden:

a) Festlegung der Anforderungen an die Informationssicherheit, die bei Informations- und Kommunikationstechnologie-Produkten oder dem Ankauf von Diensten zusätzlich zu den allgemeinen Anforderungen an die Informationssicherheit bei Lieferantenbeziehungen Anwendung finden;

b) Anforderungen an die Lieferanten von Informations- und Kommunikationstechnologie-Produkten, die Sicherheitsanforderungen der Organisation innerhalb der gesamten Lieferkette weiterzugeben für den Fall, dass die Lieferanten Unterlieferanten für Teile der Informations- und Kommunikationstechnolgie beauftragen, die für die Organisation bereitgestellt werden;

c) Anforderungen an die Lieferanten von Informations- und Kommunikationstechnologie-Produkten, entsprechende Sicherheitspraktiken innerhalb der gesamten Lieferkette weiterzugeben für den Fall, dass diese Produkte Komponenten beinhalten, die von anderen Lieferanten zugekauft wurden;

d) Implementierung eines Überwachungsprozesses sowie geeigneter Methoden zur Sicherstellung, dass die bereitgestellten Informations- und Kommunikationstechnologie-Produkte den festgelegten Sicherheitsanforderungen entsprechen;

e) Implementierung eines Prozesses zur Festlegung von Produkt- oder Dienstkomponenten, die zur Aufrechterhaltung der Funktion wesentlich sind und daher einer besonderen Aufmerksamkeit und Prüfung bedürfen, wenn sie außerhalb der Organisation erstellt werden, insbesondere wenn der führende Lieferant bestimmte Aspekte der Produkt- oder Dienstkomponenten an andere Lieferanten untervergibt;

f) Einholen der Zusicherung, dass kritische Komponenten und ihr Ursprung über die gesamte Lieferkette verfolgt werden können;

g) Einholen der Zusicherung, dass die bereitgestellten Informations- und Kommunikationstechnologie-Produkte wie erwartet funktionieren und keine unerwarteten oder unerwünschten Eigenschaften aufweisen;

h) Festlegung von Regeln für die Mitteilung von Informationen bezüglich der Lieferkette und möglicher Probleme und Kompromisse zwischen der Organisation und den Lieferanten;

i) Implementierung spezifischer Prozesse für das Management des Lebenszyklus und der Verfügbarkeit von Komponenten der Informations- und Kommunikationstechnologie sowie der damit verbundenen Sicherheitsrisiken, Dazu gehört der Umgang mit Risiken durch Komponenten, die nicht mehr erhältlich sind, da deren Anbieter nicht mehr geschäftlich tätig sind oder diese Komponenten aufgrund des technischen Fortschritts nicht mehr bereitstellen.

Weitere Informationen

Die spezifischen Risikomanagementpraktiken für die Informations- und Kommunikationstechnologie-Lieferkette bauen auf den allgemeinen Informationssicherheits-, Qualitäts-, Projektmanagement- und Systementwicklungspraktiken auf, ersetzen diese jedoch nicht.

Den Organisationen wird geraten, mit Lieferanten zusammenzuarbeiten, die über ein genaues Verständnis der Informations- und Kommunikationstechnologie-Lieferkette sowie jedweder Angelegenheiten verfügen, die Einfluss auf die bereitgestellten Produkte und Dienste haben. Die Organisationen können Einfluss auf die innerhalb der Informations- und Kommunikationstechnologie-Lieferkette angewendeten Sicherheitspraktiken nehmen, indem sie in den Verträgen mit ihren Lieferanten deutlich machen, auf welche Aspekte die anderen Lieferanten innerhalb der Informations- und Kommunikationstechnologie-Lieferkette eingehen sollten.

Die hier behandelte Informations- und Kommunikationstechnologie-Lieferkette umfasst auch Cloud-Computing-Dienste.

15.2 Management der Dienstleistungserbringung durch Lieferanten

Zielsetzung: Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit und Dienstleistungserbringung im Einklang mit Lieferantenverträgen.

15.2.1 Überwachung und Prüfung von Lieferantendienstleistungen

Maßnahme

Organisationen sollten die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, prüfen und auditieren.

Umsetzungshinweise

Mit der Überwachung und Prüfung der Lieferantendienstleistungen sollte sichergestellt werden, dass die die Informationssicherheit betreffenden Bedingungen und Konditionen des Vertrags eingehalten werden und dass Informationssicherheitsvorfälle und -probleme angemessen gehandhabt werden.

Dazu sollte ein Dienstleistungsmanagementprozess in der Beziehung zwischen der Organisation und dem Lieferanten gehören, der die folgenden Punkte umfasst:

a) Überwachung der Dienstleistungserbringungsniveaus zur Verifizierung der Vertragseinhaltung;

b) Überprüfung der vom Lieferanten vorgelegten Dienstleistungsberichte und Organisation der nach den Verträgen erforderlichen, regelmäßigen Fortschrittsbesprechungen;

c) Durchführung von Lieferanten-Audits in Verbindung mit der Überprüfung der ggf. verfügbaren Auditorberichte sowie Nachverfolgung der festgestellten Probleme;

d) Bereitstellung von Informationen zu Informationssicherheitsvorfällen und Überprüfung dieser Informationen entsprechend der vertraglichen Anforderungen sowie jedweder unterstützenden Leitlinien und Verfahren;

e) Überprüfung der Lieferanten-Prüfpfade und der Aufzeichnungen zu Informationssicherheitsereignissen, betrieblichen Problemen, Ausfällen, Fehler-Nachverfolgungen und Unterbrechungen in Bezug auf die erbrachten Dienstleistungen;

f) Lösung von und Umgang mit jedweden festgestellten Problemen;

g) Überprüfung von Aspekten der Informationssicherheit bei den Beziehungen des Lieferanten zu seinen eigenen Lieferanten;

h) Sicherstellung, dass der Lieferant eine ausreichende Leistungsfähigkeit bei der Dienstleistungserbringung aufweist, zusammen mit umsetzbaren Plänen, die darauf ausgelegt sind, sicherzustellen, dass das vereinbarte Niveau der Dienstleistungsfortführung nach schwerwiegenden Dienstleistungsausfällen oder Schäden (siehe 17) eingehalten wird.

Die Verantwortung für das Management der Lieferantenbeziehungen sollte einer dazu eigens bestimmten Person oder einem Dienstleistungsmanagement-Team übertragen werden. Zusätzlich sollte die Organisation sicherstellen, dass die Lieferanten Zuständigkeiten für die Überprüfung der Einhaltung und Durchsetzung der vertraglichen Anforderungen festlegen. Es sollten ausreichende technische Kenntnisse und Ressourcen zur Verfügung gestellt werden, um die Einhaltung der vertraglichen Anforderungen zu überwachen. Dies gilt insbesondere für die Informationssicherheitsanforderungen. Bei Feststellung von Defiziten bei der Dienstleistungserbringung sollten geeignete Maßnahmen ergriffen werden.

Die Organisation sollte für eine ausreichende Kontrolle und Transparenz hinsichtlich sämtlicher Sicherheitsaspekte bezüglich sensibler oder kritischer Informationen oder informationsverarbeitender Einrichtungen sorgen, auf die von einem Lieferanten zugegriffen, die von diesem verarbeitet oder die von ihm verwaltet werden. Die Organisation sollte mittels eines festgelegten Berichterstattungsprozesses für Transparenz in Bezug auf sicherheitsrelevante Aktivitäten wie Änderungsmanagement, Ermittlung von Schwachstellen sowie Berichterstattung über Informationssicherheitsvorfälle und die Reaktion darauf sorgen.

15.2.2 Management von Änderungen an Lieferantendienstleistungen

Maßnahme

Das Management von Änderungen an der Erbringung von Dienstleistungen durch Lieferanten, einschließlich der Pflege und Verbesserung bestehender Informationssicherheitsleitlinien, -verfahren und -kontrollen, sollte unter Berücksichtigung der Betriebswichtigkeit der betroffenen geschäftlichen Informationen, Systeme und Prozesse sowie einer erneuten Risikobewertung erfolgen.

Umsetzungshinweise

Die folgenden Aspekte sollten berücksichtigt werden:

a) Änderungen an den Lieferantenverträgen;

b) von der Organisation vorgenommene Änderungen zur Implementierung von:

   1) Verbesserungen der derzeit bereitgestellten Dienstleistungen;

   2) Weiterentwicklungen jedweder neuer Anwendungen und Systeme;

   3) Modifikationen oder Aktualisierungen in Bezug auf die Leitlinien und Verfahren der Organisationen;

   4) neuen oder veränderten Kontrollmaßnahmen zur Klärung von Informationssicherheitsvorfällen und zur Verbesserung der Sicherheit;

c) Änderungen an den Lieferantendienstleistungen zur Implementierung:

   1) von Änderungen und Verbesserungen an den Netzwerken;

2) zur Nutzung neuer Technologien;

3) zur Einführung neuer Produkte oder neuerer Versionen/Releases;

4) neuer Entwicklungswerkzeuge und -umgebungen;

5) von Änderungen am Standort der Dienstleistungseinrichtungen;

6) von Lieferantenwechseln;

7) von Untervertragsvergaben an andere Lieferanten.

16 Management von Informationssicherheitsvorfällen

16.1 Management von Informationssicherheitsvorfällen und Verbesserungen

Zielsetzung: Sicherstellung einer konsistenten und wirksamen Strategie für das Management von Informationssicherheitsvorfällen, einschließlich der Kommunikation über Sicherheitsereignisse und -schwachstellen.

16.1.1 *Zuständigkeiten und Verfahren*

Maßnahme

Es sollten Managementverantwortlichkeiten und -verfahren festgelegt werden, um eine schnelle, wirksame und ordnungsgemäße Reaktion auf Informationssicherheitsvorfälle sicherzustellen.

Umsetzungshinweise

Die folgenden Leitlinien zu Managementverantwortlichkeiten und -verfahren hinsichtlich des Umgangs mit Informationssicherheitsvorfällen sollten berücksichtigt werden:

a) Es sollten Managementverantwortlichkeiten festgelegt werden, um sicherzustellen, dass die folgenden Verfahren entwickelt und angemessen innerhalb der Organisation kommuniziert werden:

   1) Verfahren für Planung und Vorbereitung von Abhilfemaßnahmen bei Vorfällen;

   2) Verfahren zur Überwachung, Erkennung, Analyse sowie zur Berichterstattung über Informationssicherheitsereignisse und -vorfälle;

   3) Verfahren zur Protokollierung von Vorfallsmanagementaktivitäten;

   4) Verfahren zum Umgang mit forensischem Beweismaterial;

   5) Verfahren zur Beurteilung von und zur Entscheidung über Informationssicherheitsereignisse(n) sowie Beurteilung von Schwachstellen bezüglich der Informationssicherheit;

   6) Reaktionsverfahren einschließlich jener zur Eskalation, kontrollierten Wiederherstellung nach einem Vorfall sowie zur Kommunizierung an relevante, interne und externe Personen oder Organisationen;

b) Es sollten Verfahren festgelegt werden, durch die Folgendes sichergestellt wird:

1) Angelegenheiten in Bezug auf Informationssicherheitsvorfälle innerhalb der Organisation werden von kompetenten Mitarbeitern bearbeitet;

2) Es wird ein Ansprechpartner für die Erkennung von Sicherheitsvorfällen und die Berichterstattung bestimmt;

3) Es werden entsprechende Kontakte mit den Behörden, externen Interessengruppen oder Foren unterhalten, die Angelegenheiten in Bezug auf Informationssicherheitsvorfälle behandeln;

c) Es existieren Berichterstattungsverfahren, die folgende Punkte beinhalten:

1) Vorbereitung von Formularen für die Berichterstattung über Informationssicherheitsereignisse zur Unterstützung der Berichterstattungsanstrengungen, damit die Bericht erstattenden Personen im Fall eines Informationssicherheitsereignisses an alle erforderlichen Maßnahmen denken;

2) das im Fall eines Informationssicherheitsereignisses zu verwendende Verfahren, z. B. unverzügliches Notieren aller Details (z. B. Art der Nichteinhaltung bzw. des Verstoßes, auftretende Fehlfunktion, Bildschirmmeldungen, seltsames Verhalten), keine eigenmächtige Durchführung von Maßnahmen, sondern unverzügliche Berichterstattung an den Ansprechpartner und lediglich Ergreifung koordinierter Maßnahmen;

3) Bezugnahme auf ein festgelegtes, formelles Disziplinarverfahren zum Umgang mit Mitarbeitern, die gegen die Sicherheitsbestimmungen verstoßen;

4) geeignete Rückmeldungsprozesse, um sicherzustellen, dass Personen, die Informationssicherheitsereignisse berichten, nach Abschluss der Vorfallsbehandlung benachrichtigt werden.

Die Ziele des Umgangs mit Informationssicherheitsvorfällen sollten mit dem Management abgestimmt werden, und es sollte sichergestellt werden, dass den für den Umgang mit Informationssicherheitsvorfällen verantwortlichen Personen die Prioritäten der Organisation beim Umgang mit Informationssicherheitsvorfällen bekannt sind.

Weitere Informationen

Informationssicherheitsvorfälle können organisations- und staatenübergreifende Auswirkungen haben. Beim Umgang mit derartigen Vorfällen besteht ein zunehmender Bedarf zur Koordinierung betreffender Gegenmaßnahmen sowie ggf. zum Informationsaustausch über diese Vorfälle mit externen Organisationen.

Eine ausführliche Anleitung zum Umgang mit Informationssicherheitsvorfällen kann ISO/IEC 27035 entnommen werden.

16.1.2 Meldung von Informationssicherheitsereignissen

Maßnahme

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

Umsetzungshinweise

Alle Mitarbeiter und Auftragnehmer sollten auf ihre Verantwortung hingewiesen werden, Informationssicherheitsereignisse so schnell wie möglich zu melden. Sie sollten das Verfahren zur Berichterstattung über Informationssicherheitsereignisse kennen sowie den Ansprechpartner, an den die Ereignisse zu berichten sind.

Zu den Situationen, die bei der Berichterstattung über Informationssicherheitsereignisse zu berücksichtigen sind, zählen:

a) unwirksame Sicherheitsmaßnahmen;

b) Verstöße gegen die erwartete Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen;

c) menschliches Versagen;

d) Nichteinhaltung von Richtlinien oder Leitlinien;

e) Verstöße gegen physische Sicherungsvorkehrungen;

f) unkontrollierte Systemänderungen;

g) Fehlfunktionen von Software oder Hardware;

h) Zugriffsverstöße.

Weitere Informationen

Fehlfunktionen oder sonstiges abweichendes Systemverhalten können ein Anzeichen für einen Angriff auf die Systemsicherheit sein und sollten daher immer als Informationssicherheitsereignis berichtet werden.

16.1.3 Meldung von Informationssicherheitsschwachstellen

Maßnahme

Mitarbeiter und Auftragnehmer, die die Informationssysteme und -dienste der Organisation nutzen, sollten dazu aufgefordert werden, jegliche beobachteten oder vermuteten Informationssicherheitsschwachstellen in Systemen oder Diensten festzuhalten und zu melden.

Umsetzungshinweise

Alle Mitarbeiter und Auftragnehmer sollten diese Angelegenheiten so schnell wie möglich dem Ansprechpartner melden, um das Auftreten von Informationssicherheitsvorfällen zu verhindern. Der Berichterstattungsmechanismus sollte so einfach, zugänglich und verfügbar wie möglich gehalten werden.

Weitere Informationen

Mitarbeitern und Auftragnehmern sollte abgeraten werden, einen Versuch zum Nachweis der vermuteten Sicherheitsschwachstellen zu unternehmen. Das Austesten von Schwachstellen kann als potenzielle Fehlanwendung des Systems interpretiert werden und zudem zu Schäden am Informationssystem oder Dienst führen sowie eine rechtliche Haftung der ausführenden Person nach sich ziehen.

16.1.4 Bewertung von und Entscheidung über Informationssicherheitsereignisse

Maßnahme

Informationssicherheitsereignisse sollten bewertet werden, und es sollte darüber entschieden werden, ob sie als Informationssicherheitsvorfälle einzustufen sind.

Umsetzungshinweise

Der Ansprechpartner sollte jedes Informationssicherheitsereignis mittels des vereinbarten Klassifizierungsschemas für Informationssicherheitsereignisse und -vorfälle bewerten und entscheiden, ob das Ereignis als Vorfall eingestuft werden sollte. Die Klassifizierung und Priorisierung von Vorfällen kann helfen, die Auswirkungen und das Ausmaß eines Vorfalls festzustellen.

In Fällen, in denen die Organisation über ein Interventionsteam für Informationssicherheitsvorfälle (Information Security Incident Response Team, ISIRT) verfügt, kann die Bewertung und Entscheidung an das ISIRT zur Bestätigung oder Neubewertung weitergeleitet werden.

Die Ergebnisse der Bewertung und Entscheidung sollten ausführlich aufgezeichnet werden, damit später zur Verifizierung darauf zurückgegriffen werden kann.

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Maßnahme

Auf Informationssicherheitsvorfälle sollte entsprechend den dokumentierten Verfahren reagiert werden.

Umsetzungshinweise

Auf Informationssicherheitsvorfälle sollte von einem dazu bestimmten Ansprechpartner und anderen relevanten Personen der Organisation oder externer Parteien (siehe 16.1.1) reagiert werden.

Die Reaktion sollte die folgenden Punkte umfassen:

a) möglichst frühzeitiges Sichern von Beweismaterial nach dem Vorkommnis;

b) Durchführung einer forensischen Informationssicherheitsanalyse, sofern erforderlich (siehe 16.1.7);

c) Eskalation, sofern erforderlich;

d) Sicherstellung, dass alle durchgeführten Abhilfeaktivitäten zur späteren Analyse ordnungsnach protokolliert werden;

e) Kommunizierung des aufgetretenen Informationssicherheitsvorfalls bzw. jedweder relevanter Details an andere interne oder externe Personen oder Organisationen, die davon Kenntnis erhalten müssen;

f) Umgang mit Informationssicherheitsschwachstellen, die als ursächlich oder begünstigend für den Vorfall festgestellt wurden;

g) formeller Abschluss und Dokumentierung nach erfolgreichem Abschluss der Vorfallsbehandlung.

Nach dem Vorfall sollte ggf. eine Analyse stattfinden, um die Vorfallsursache festzustellen.

Weitere Informationen

Das erste Ziel der Abhilfemaßnahmen bei Vorfällen besteht darin, das „normale Sicherheitsniveau“ wiederherzustellen und danach die notwendige Wiederherstellung einzuleiten.

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Maßnahme

Aus der Analyse und Lösung von Informationssicherheitsvorfällen gewonnene Erkenntnisse sollten dazu genutzt werden, die Auftretenswahrscheinlichkeit oder die Auswirkungen zukünftiger Vorfälle zu verringern.

Umsetzungshinweise

Es sollten Mechanismen existieren, um Art, Umfang und Kosten von Informationssicherheitsvorfällen zu quantifizieren und zu überwachen. Die durch die Bewertung von Informationssicherheitsvorfällen erhaltenen Informationen sollten dazu verwendet werden, wiederkehrende Vorfälle oder Vorfälle mit schwerwiegenden Auswirkungen zu ermitteln.

Weitere Informationen

Die Bewertung von Informationssicherheitsvorfällen kann die Notwendigkeit für erweiterte oder zusätzliche Kontrollmaßnahmen zur Begrenzung der Häufigkeit, des Schadenspotenzials und der Kosten zukünftig auftretender Vorfälle ergeben oder der Berücksichtigung im Rahmen des Überprüfungsprozesses vor dem Hintergrund der Sicherheitsleitlinie (siehe 5.1.2).

Unter gebührender Berücksichtigung der Vertraulichkeit können Vorkommnisse aus Informationssicherheitsvorfällen, die sich tatsächlich zugetragen haben, im Rahmen der Benutzersensibilisierungsschulung (siehe 7.2.2) als Beispiele möglicher Szenarios, daraufhin zu ergreifender Abhilfemaßnahmen und Vorkehrungen zur zukünftigen Verhinderung verwendet werden.

16.1.7 Sammeln von Beweismaterial

Maßnahme

Die Organisation sollte Verfahren für die Ermittlung, Sammlung, Aneignung und Aufbewahrung von Informationen, die als Beweismaterial dienen können, festlegen und anwenden.

Umsetzungshinweise

Es sollten interne Verfahren zum Umgang mit Beweismaterial für Disziplinarmaßnahmen und gerichtliche Schritte entwickelt und angewendet werden.

Allgemein sollten diese Beweisverfahren Verfahren zur Ermittlung, Sammlung, Aneignung und Aufbewahrung von Beweismaterial entsprechend den verschiedenen Arten von Medien, Geräten und Gerätestatus (z. B. ein- oder ausgeschaltet) bereitstellen. Bei den Verfahren sollten folgende Punkte berücksichtigt werden:

a) Kontrollkette;

b) Sicherheit des Beweismaterials;

c) Sicherheit der Mitarbeiter;

d) Aufgaben und Zuständigkeiten der involvierten Mitarbeiter;

e) Kompetenz der Mitarbeiter;

f) Dokumentation;

g) Einweisung.

Sofern verfügbar, sollte auf Zertifizierungen oder andere relevante Qualifizierungsmittel für Mitarbeiter und Werkzeuge zurückgegriffen werden, um den Wert des aufbewahrten Beweismaterials zu unterstreichen.

Forensisches Beweismaterial kann mehrere Organisationen oder Rechtsordnungen berühren. In derartigen Fällen sollte sichergestellt werden, dass die Organisation befugt ist, die erforderlichen Informationen als forensisches Beweismaterial zu sammeln. Außerdem sollten die Anforderungen der verschiedenen Rechtsordnungen beachtet werden, damit die Wahrscheinlichkeit der rechtsordnungsübergreifenden Anerkennung möglichst groß ist.

Weitere Informationen

Unter „Ermittlung“ wird der Prozess der Suche nach sowie der Anerkennung und der Dokumentation von potenziellem Beweismaterial verstanden. Unter „Sammlung“ wird der Prozess der Erfassung der physischen Gegenstände verstanden, die potenzielles Beweismaterial enthalten können. Unter „Aneignung“ wird der Prozess der Erstellung einer Kopie der Daten innerhalb eines festgelegten Satzes verstanden. Unter „Aufbewahrung“ wird der Prozess der Erhaltung und des Schutzes der Integrität und des ursprünglichen Zustands des potenziellen Beweismaterials verstanden.

Bei Erkennung eines Informationssicherheitsereignisses ist möglicherweise nicht sofort absehbar, ob das Ereignis zu einem gerichtlichen Vorgehen führen wird. Daher besteht die Gefahr, dass notwendiges Beweismaterial vorsätzlich oder versehentlich zerstört wird, bevor die Schwere des Vorfalls erkannt wurde. Es ist ratsam, beim Erwägen rechtlicher Schritte frühzeitig einen Rechtsanwalt oder die Polizei hinzuzuziehen und einen Rat bezüglich des erforderlichen Beweismaterials einzuholen.

ISO/IEC 27037 enthält Leitlinien zur Ermittlung, Sammlung, Aneignung und Aufbewahrung digitalen Beweismaterials.

17 Informationssicherheitsaspekte des Betriebskontinuitätsmanagements

17.1 Aufrechterhaltung der Informationssicherheit

Zielsetzung: Die Aufrechterhaltung der Informationssicherheit sollte in die Betriebskontinuitäts-managementsysteme der Organisation eingebettet sein.

17.1.1 Planung der Aufrechterhaltung der Informationssicherheit

Maßnahme

Die Organisation sollte ihre Anforderungen bezüglich der Informationssicherheit und für die Aufrechterhaltung des Informationssicherheitsmanagements in schwierigen Situationen wie z. B. in einem Krisen- oder Schadensfall festlegen.

Umsetzungshinweise

Die Organisation sollte festlegen, ob die Aufrechterhaltung der Informationssicherheit im Rahmen des Betriebskontinuitätsmanagementprozesses oder innerhalb eines Notfallwiederherstellungsmanagement-prozesses berücksichtigt werden soll. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Falls keine formelle Planung zur Betriebskontinuität und Notfallwiederherstellung existiert, sollten die Informationssicherheitsanforderungen unter normalen Betriebsbedingungen auch in schwierigen Situationen zur Anwendung kommen. Alternativ kann die Organisation eine Analyse der geschäftlichen Auswirkungen in Bezug auf Aspekte der Informationssicherheit durchführen, um die Informationssicherheitsanforderungen zu bestimmen, die für schwierige Situationen gelten sollen.

Weitere Informationen

Zur Begrenzung der für eine „zusätzliche“ Analyse der geschäftlichen Auswirkungen in Bezug auf Informationssicherheit benötigten Zeit und des entsprechenden Aufwands wird empfohlen, die Informations-sicherheitsaspekte innerhalb der normalen Analyse der geschäftlichen Auswirkungen im Rahmen des Betriebskontinuitätsmanagements oder des Notfallwiederherstellungsmanagement zu erfassen. Dies setzt voraus, dass die Anforderungen bezüglich der Aufrechterhaltung der Informationssicherheit ausdrücklich in den Prozessen zum Betriebskontinuitätsmanagement oder Notfallwiederherstellungsmanagement formuliert sind.

Informationen zum Betriebskontinuitätsmanagement können ISO/IEC 27031, ISO/IEC 22313 und ISO/IEC 22301 entnommen werden.

17.1.2 Implementierung von Verfahren zur Aufrechterhaltung der Informationssicherheit

Maßnahme

Die Organisation sollte Prozesse, Verfahren und Kontrollmaßnahmen festlegen, dokumentieren, implementieren und aufrechterhalten, um das erforderliche Maß an Kontinuität der Informationssicherheit in einer schwierigen Situation sicherzustellen.

Umsetzungshinweise

Eine Organisation sollte folgende Punkte sicherstellen:

a) Vorhandensein einer angemessenen Verwaltungsstruktur zur Vorbereitung, Eindämmung und Reaktion in Bezug auf ein störendes Ereignis unter Rückgriff auf Mitarbeiter mit der erforderlichen Befugnis, Erfahrung und Kompetenz;

b) Bestimmung von Mitarbeitern für Reaktionsmaßnahmen, die über die nötige Verantwortung, Befugnis und Kompetenz zum Umgang mit Vorfällen und zur Aufrechterhaltung der Informationssicherheit verfügen;

c) Entwicklung und Genehmigung dokumentierter Pläne, Reaktions- und Wiederherstellungsverfahren, in denen genau festgelegt ist, wie die Organisation mit einem störenden Ereignis umgeht und die Informationssicherheit auf einem vorher festgelegten Niveau auf Grundlage der vom Management genehmigten Ziele zur Aufrechterhaltung der Informationssicherheit sicherstellt (siehe 17.1.1).

Entsprechend den Anforderungen bezüglich der Aufrechterhaltung der Informationssicherheit sollte die Organisation die folgenden Punkte festlegen, dokumentieren, implementieren bzw. aufrechterhalten:

a) Informationssicherheitsmaßnahmen innerhalb der Betriebskontinuitäts- oder Notfallwiederherstellungsprozesse und -verfahren sowie der unterstützenden Systeme und Werkzeuge;

b) Prozesse, Verfahren und Umsetzungsänderungen zur Aufrechterhaltung der bestehenden Informationssicherheitsmaßnahmen in einer schwierigen Situation;

c) Kompensierung von Kontrollen für Informationssicherheitsmaßnahmen, die in einer schwierigen Situation nicht aufrechterhalten werden können.

Weitere Informationen

Im Kontext von Betriebskontinuität oder Notfallwiederherstellung können spezifische Prozesse und Verfahren festgelegt worden sein. Informationen, mit denen im Rahmen dieser Prozesse und Verfahren oder innerhalb eigener Informationssysteme zu deren Unterstützung umgegangen wird, sollten geschützt werden. Daher sollte eine Organisation Informationssicherheitsspezialisten hinzuziehen, wenn es um die Einrichtung, Implementierung und Aufrechterhaltung von Prozessen und Verfahren zur Sicherstellung der Betriebskontinuität und der Notfallwiederherstellung geht.

Informationssicherheitsmaßnahmen, die bereits implementiert wurden, sollten in einer schwierigen Situation in Betrieb bleiben. Falls die Sicherheitsmaßnahmen die Informationen nicht mehr schützen können, sollten andere Maßnahmen festgelegt, implementiert und aufrechterhalten werden, um eine ausreichende Informationssicherheit zu gewährleisten.

17.1.3 Überprüfung, Überarbeitung und Auswertung von Maßnahmen zur Aufrechterhaltung der Informationssicherheit

Maßnahme

Die Organisation sollte die festgelegten und implementierten Kontrollmaßnahmen zur Aufrechterhaltung der Informationssicherheit in regelmäßigen Abständen überprüfen, um sicherzustellen, dass sie gültig und auch in schwierigen Situationen wirksam sind.

Umsetzungshinweise

Änderungen in der Organisation, der Technik, Verfahren und Prozesse im betrieblichen Kontext als auch im Zusammenhang mit der Betriebskontinuität, können zu veränderten Anforderungen hinsichtlich der Anforderungen bezüglich der Aufrechterhaltung der Informationssicherheit führen. In derartigen Fällen sollte die Aufrechterhaltung der Prozesse, Verfahren und Kontrollmaßnahmen in Bezug auf die Informationssicherheit vor dem Hintergrund dieser veränderten Anforderungen überprüft werden.

Die Organisationen sollten die Aufrechterhaltung ihres Informationssicherheitsmanagements folgendermaßen überprüfen:

a) Verwendung und Überprüfung der Funktion der Prozesse, Verfahren und Kontrollmaßnahmen zur Aufrechterhaltung der Informationssicherheit, um sicherzustellen, dass diese den Zielen zur Aufrechterhaltung der Informationssicherheit entsprechen;

b) Anwendung und Überprüfung der Kenntnisse und Routine zum Betrieb der Prozesse, Verfahren und Kontrollmaßnahmen zur Aufrechterhaltung der Informationssicherheit, um sicherzustellen, dass deren Leistung den Zielen zur Aufrechterhaltung der Informationssicherheit entspricht;

c) Überprüfung der Gültigkeit und Wirksamkeit der Maßnahmen zur Aufrechterhaltung der Informationssicherheit bei Änderungen an den Informationssystemen, den Prozesse, Verfahren und Kontrollmaßnahmen zur Gewährleistung der Informationssicherheit oder den Prozessen und Lösungen im Zusammenhang mit dem Betriebskontinuitätsmanagement/der Notfallwiederherstellung.

Weitere Informationen

Die Überprüfung der Kontrollmaßnahmen zur Aufrechterhaltung der Informationssicherheit unterscheidet sich von der allgemeinen Überprüfung und Verifizierung der Informationssicherheit und sollte unabhängig von der Überprüfung von Änderungen durchgeführt werden. Die Überprüfung der Kontrollmaßnahmen zur Aufrechterhaltung der Informationssicherheit sollte vorzugsweise in die Prüfungen der Betriebskontinuität oder der Notfallwiederherstellung der Organisation integriert werden.

17.2 Redundanzen

Zielsetzung: Sicherstellung der Verfügbarkeit von informationsverarbeitenden Einrichtungen.

17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

Maßnahme

Informationsverarbeitende Einrichtungen sollten mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen implementiert werden.

Umsetzungshinweise

Die Organisationen sollten die geschäftlichen Anforderungen für die Verfügbarkeit von Informationssystemen feststellen. Wenn die Verfügbarkeit nicht mittels der bestehenden Systemarchitektur gewährleistet werden kann, sollten redundante Komponenten oder Architekturen in Betracht gezogen werden.

Vorhandene redundante Informationssysteme sollten überprüft werden, um sicherzustellen, dass beim Ausfall einer Komponente die redundante Komponente wie beabsichtigt funktioniert.

Weitere Informationen

Die Umsetzung von Redundanzen kann zu Risiken für die Integrität oder Vertraulichkeit der Informationen und Informationssysteme führen, die beim Entwurf der Informationssysteme zu berücksichtigen sind.

18 Richtlinienkonformität

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

Zielsetzung: Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit sowie gegen jegliche Sicherheitsanforderungen.

18.1.1 Feststellung anwendbarer Gesetze und vertraglicher Anforderungen

Maßnahme

Alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen sowie die Strategie der Organisation zur Erfüllung dieser Anforderungen sollten für jedes Informationssystem sowie für die Organisation ausdrücklich ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.

Umsetzungshinweise

Die spezifischen Maßnahmen und die einzelnen Zuständigkeiten zur Erfüllung dieser Anforderungen sollten ebenfalls festgelegt und dokumentiert werden.

Das Management sollte alle für ihre Organisation geltenden Gesetze ermitteln, um alle ihre geschäftliche Tätigkeit betreffenden Anforderungen zu erfüllen. Wenn die Organisation auch in anderen Ländern geschäftlich tätig ist, sollte das Management darauf achten, dass die Richtlinienkonformität auch für diese Länder sichergestellt ist.

18.1.2 Rechte an geistigem Eigentum

Maßnahme

Es sollten geeignete Verfahren umgesetzt werden, um die Einhaltung aller gesetzlichen, behördlichen und vertraglichen Anforderungen in Bezug auf die geistigen Eigentumsrechte an und die Nutzung von urheberrechtlich geschützten Software-Produkten sicherzustellen.

Umsetzungshinweise

Die folgenden Leitlinien sollten zum Schutz von jedwedem Material berücksichtigt werden, welches möglicherweise als geistiges Eigentum betrachtet wird:

a) Veröffentlichung einer Richtlinie zur Einhaltung geistiger Eigentumsrechte, in der die legale Nutzung von Software- und Informationsprodukten geregelt wird;

b) Bezug von Software nur über bekannte und seriöse Quellen, um sicherzustellen, dass das Urheberrecht nicht verletzt wird;

c) nachhaltige Sensibilisierung für die Richtlinien zum Schutz geistiger Eigentumsrechte und Benachrichtigung über die Absicht, Disziplinarmaßnahmen gegen Mitarbeiter zu ergreifen, die dagegen verstoßen;

d) Führen entsprechender Anlagenregister und Feststellung aller Anlagen und Werte mit Schutzanforderungen bezüglich der geistigen Eigentumsrechte;

e) Aufbewahrung von Nachweisen und Beweismaterial für die Inhaberschaft von Lizenzen, Originaldatenträgern, Handbüchern usw.;

f) Implementierung von Kontrollmaßnahmen, um sicherzustellen, dass die in den Lizenzbedingungen festgelegte maximale Nutzerzahl nicht überschritten wird;

g) Durchführung von Überprüfungen, um sicherzustellen, dass nur genehmigte Software und lizenzierte Produkte installiert sind;

h) Bereitstellung einer Richtlinie zur Einhaltung der entsprechenden Lizenzbedingungen;

i) Bereitstellung einer Richtlinie zur Veräußerung bzw. Übertragung von Software an andere;

j) Einhaltung der Bedingungen und Konditionen in Bezug auf Software und Informationen, die aus öffentlichen Netzen stammen;

k) keine Vervielfältigung, Formatkonvertierung oder Verwendung von Auszügen kommerzieller Aufzeichnungen (Film oder Ton), die nach dem Urheberrecht untersagt ist;

l) keine Anfertigung von vollständigen oder auszugsweisen Kopien von Büchern, Artikeln, Berichten oder anderen Dokumenten, die nach dem Urheberrecht untersagt ist.

Weitere Informationen

Die geistigen Eigentumsrechte beinhalten das Urheberrecht an Software und Dokumenten, Geschmacksmustern, Markenzeichen, Patente und Quellcode-Lizenzen.

Urheberrechtlich geschützte Software-Produkte unterliegen üblicherweise einer Lizenzvereinbarung, in der die Lizenzbedingungen festgelegt sind, die beispielsweise die Nutzung der Produkte auf bestimmte Geräte beschränken oder nur die Vervielfältigung zur Erstellung von Backup-Kopien gestatten. Die Wichtigkeit des Themas der geistigen Eigentumsrechte und die Sensibilisierung dafür sollte gegenüber den Mitarbeitern in Bezug auf Software kommuniziert werden, die innerhalb der Organisation entwickelt wird.

Rechtliche, behördliche und vertragliche Anforderungen können Beschränkungen bezüglich des Kopierens urheberrechtlich geschützten Materials beinhalten. Insbesondere kann die Anforderung existieren, dass nur Material verwendet werden darf, das von der Organisation entwickelt oder vom Entwickler an die Organisation lizenziert bzw. ihr zur Verfügung gestellt wird. Urheberrechtsverstöße können rechtliche Schritte zur Folge haben, einschließlich der Verhängung von Bußgeldern und einer strafrechtlichen Verfolgung.

18.1.3 Schutz von Aufzeichnungen

Maßnahme

Aufzeichnungen sollten nach den gesetzlichen, behördlichen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, nicht autorisiertem Zugriff und nicht autorisierter Freigabe geschützt werden.

Umsetzungshinweise

Bei der Entscheidung über den Schutz bestimmter Aufzeichnungen der Organisation sollten die entsprechenden Klassifizierungen auf Grundlage des Klassifizierungsschemas der Organisation berücksichtigt werden. Die Aufzeichnungen sollten nach Aufzeichnungsarten kategorisiert werden, z. B. Geschäftsbücher, Datenbanksätze, Transaktionsprotokolle, Audit-Protokolle und Betriebsverfahren, jeweils mit Angabe von Einzelheiten zu Aufbewahrungszeiträumen und Art der zulässigen Speichermedien, z. B. Papier, Mikrofiche, magnetische und optische Speichermedien. Alle kryptographischen Schlüssel und Programme, die für verschlüsselte Archive oder digitale Signaturen (siehe 10) benötigt werden, sollten ebenfalls gespeichert werden, um eine Entschlüsselung der Aufzeichnungen für den Zeitraum ihrer Aufbewahrung zu ermöglichen.

Es sollte die Möglichkeit der Qualitätsminderung der für die Speicherung der Aufzeichnungen verwendeten Medien in Betracht gezogen werden. Die Verfahren zu Speicherung und Umgang sollten entsprechend den Herstellerempfehlungen implementiert werden.

Bei der Wahl elektronischer Speichermedien sollten Verfahren festgelegt werden, durch die der Zugriff auf die Daten (hinsichtlich der Lesbarkeit des Mediums als auch des Formats) über den gesamten

Aufbewahrungszeitraum sichergestellt ist, um vor Datenverlust aufgrund zukünftiger technischer Veränderungen geschützt zu sein.

Datenspeichersysteme sollten so ausgewählt werden, dass die benötigten Daten in Abhängigkeit von den zu erfüllenden Anforderungen innerhalb eines vertretbaren Zeitrahmens und im gewünschten Format abgerufen werden können.

Das Speicher- und Handhabungssystem sollte ggf. die Kennzeichnung von Aufzeichnungen und ihrer Aufbewahrungsfrist nach den Festlegungen durch nationale oder regionale Gesetze oder Verordnungen sicherstellen. Dieses System sollte die entsprechende Vernichtung von Aufzeichnungen nach Ablauf dieser Frist ermöglichen, falls die Organisation sie nicht mehr benötigt.

Zur Erreichung dieser Ziele zum Schutz der Aufzeichnungen sollten innerhalb der Organisation die folgenden Schritte unternommen werden:

a) Herausgabe von Leitlinien für die Aufbewahrung, Lagerung, Handhabung und Entsorgung von Aufzeichnungen und Informationen;

b) Erstellung einer Aufbewahrungsplanung, in der die Aufzeichnungen und deren jeweiliger Aufbewahrungszeitraum niedergelegt sind;

c) Führen eines Quellenverzeichnisses für wichtige Informationen.

Weitere Informationen

Einige Aufzeichnungen müssen zur Erfüllung gesetzlicher, behördlicher oder vertraglicher Verpflichtungen sowie zur Unterstützung zentraler geschäftlicher Aktivitäten möglicherweise sicher verwahrt werden. Dies betrifft beispielsweise Aufzeichnungen, die als Nachweis für eine den gesetzlichen und behördlichen Auflagen entsprechende Betriebstätigkeit der Organisation dienen, zur Sicherstellung der Verteidigung gegen potenzielle zivil- oder strafrechtliche Klagen oder zur Bestätigung des finanziellen Status einer Organisation gegenüber den Anteilseignern, externen Parteien oder Auditoren. Der Aufbewahrungszeitraum und der Umfang der aufzubewahrenden Informationen können durch nationale Gesetze oder Bestimmungen vorgegeben sein.

Weitere Informationen zum Umgang mit den Aufzeichnungen der Organisation können ISO 15489-1 entnommen werden.

18.1.4 Privatsphäre und Schutz von personenbezogenen Informationen

Maßnahme

Die Privatsphäre sowie der Schutz von personenbezogenen Informationen sollten entsprechend den Anforderungen der relevanten Gesetze, Vorschriften und ggf. Vertragsbestimmungen sichergestellt werden.

Umsetzungshinweise

Die Organisation sollte eine Datenrichtlinie zum Schutz der Privatsphäre und personenbezogenen Informationen entwickeln und implementieren. Diese Richtlinie sollte an alle Personen kommuniziert werden, die in die Verarbeitung personenbezogener Informationen einbezogen sind.

Zur Sicherstellung der Einhaltung dieser Richtlinie und aller relevanten Gesetze und Vorschriften zum Schutz der Privatsphäre und personenbezogener Daten ist eine entsprechende Managementstruktur und -kontrolle erforderlich. Am besten kann dies meist durch Benennung einer dafür zuständigen Person wie eines Datenschutzbeauftragten erreicht werden, der den Vorgesetzten, Benutzern und Dienstleistern eine Richtschnur hinsichtlich ihrer jeweiligen Verantwortungsbereiche sowie der jeweils einzuhaltenden Verfahren vorgibt. Die Wahrnehmung der Verantwortung für den Umgang mit personenbezogenen Informationen und die Sicherstellung der Sensibilisierung für die Prinzipien des Schutzes der Privatsphäre sollten nach den geltenden Gesetzen und Vorschriften erfolgen. Es sollten geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Informationen implementiert werden.

Weitere Informationen

ISO/IEC 29100 bietet einen groben Rahmen für den Schutz personenbezogener Informationen im Rahmen von Informations- und Kommunikationstechnologiesystemen. Einige Länder haben Gesetze zur Kontrolle der Erhebung, Verarbeitung und Übermittlung personenbezogener Daten (im Allgemeinen Informationen über lebende Personen, die anhand dieser Informationen identifiziert werden können) erlassen. In Abhängigkeit von den jeweiligen nationalen Gesetzen können derartige Kontrollen die Auferlegung bestimmter Pflichten bei der Erhebung, Verarbeitung und Weitergabe personenbezogener Daten sowie eine Einschränkung der Übermittlung in andere Länder beinhalten.

18.1.5 Regulierung kryptographischer Kontrollmaßnahmen

Maßnahme

Kryptographische Kontrollmaßnahmen sollten unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt werden.

Umsetzungshinweise

Zur Einhaltung der relevanten Vereinbarungen, Gesetze und Vorschriften sollten die folgenden Punkte berücksichtigt werden:

a) Beschränkungen bezüglich des Im- oder Exports von Computer-Hardware und -Software zur Durchführung kryptographischer Funktionen;

b) Beschränkungen bezüglich des Im- oder Exports von Computer-Hardware und -Software, die für die Hinzufügung kryptographischer Funktionen ausgelegt ist;

c) Beschränkungen bezüglich der Anwendung von Verschlüsselungstechnologien;

d) verpflichtende oder freiwillige Methoden für den Zugriff der Behörden des Landes auf hardware- oder softwareseitig verschlüsselte Informationen zur Gewährleistung der Rechtskonformität der Inhalte.

Es sollte eine Rechtsberatung in Anspruch genommen werden, um die Einhaltung aller relevanten Gesetze und Vorschriften sicherzustellen. Vor der Übermittlung verschlüsselter Informationen oder kryptographischer Maßnahmen über geografische Geltungsgrenzen der anzuwendenden Gesetze und Vorschriften hinweg sollte ebenfalls eine Rechtsberatung in Anspruch genommen werden.

18.2 Informationssicherheitsprüfungen

Zielsetzung: Sicherstellung, dass Informationssicherheitsvorkehrungen entsprechend den Leitlinien und Verfahren der Organisation implementiert und angewandt werden.

18.2.1 Unabhängige Prüfung der Informationssicherheit

Maßnahme

Die Strategie der Organisation für das Management der Informationssicherheit und deren Implementierung (d. h. Kontrollziele und -maßnahmen, Leitlinien, Prozesse und Verfahren zur Informationssicherheit) sollten in planmäßigen Abständen oder jeweils bei erheblichen Änderungen an der Implementierung von Sicherheitsvorkehrungen durch eine unabhängige Stelle geprüft werden.

Umsetzungshinweise

Das Management sollte die unabhängige Prüfung veranlassen. Eine derartige unabhängige Prüfung ist erforderlich, um die Eignung, Tauglichkeit und Wirksamkeit des Ansatzes der Organisation in Bezug auf das Informationssicherheitsmanagement dauerhaft sicherzustellen. Diese Prüfung sollte eine Beurteilung von Verbesserungsmöglichkeiten und ggf. vorhandenem Änderungsbedarf bezüglich des Sicherheitsansatzes einschließlich der Richtlinien- und Maßnahmenziele beinhalten.

Diese Prüfung sollte von Personen durchgeführt werden, die unabhängig vom untersuchten Bereich sind. Dabei kann es sich z. B. um einen internen Auditor, einen unabhängigen Manager oder eine externe Organisation handeln, die sich auf derartige Prüfungen spezialisiert hat. Die diese Prüfungen durchführenden Personen müssen über entsprechende Kompetenzen und Erfahrungen verfügen.

Die Ergebnisse der unabhängigen Prüfung sollten aufgezeichnet und an das Management berichtet werden, welches die Prüfung veranlasst hat. Diese Aufzeichnungen sollten aufbewahrt werden.

Sollte bei der unabhängigen Prüfung festgestellt werden, dass der Informationssicherheitsmanagement-Ansatz der Organisation und dessen Umsetzung nicht angemessen sind, weil z. B. dokumentierte Ziele und Anforderungen nicht eingehalten werden oder nicht der in den Informationssicherheitsleitlinien (siehe 5.1.1) festgelegten Richtung entsprechen, sollte das Management Korrekturmaßnahmen in Betracht ziehen.

Weitere Informationen

ISO/IEC 27007 „Richtlinien für Informationssicherheits-Managementsystemaudits“ und ISO/IEC TR 27008 „Richtlinien für Auditoren von Informationssicherheits-controls“ bieten ebenfalls eine Anleitung zur Durchführung der unabhängigen Prüfung.

18.2.2 Einhaltung von Sicherheitsleitlinien und -normen

Maßnahme

Das Management sollte regelmäßig die Konformität der Informationsverarbeitung und der Verfahren in ihrem Zuständigkeitsbereich mit den jeweils anwendbaren Sicherheitsleitlinien, Normen und jeglichen sonstigen Sicherheitsanforderungen prüfen.

Umsetzungshinweise

Das Management sollte feststellen, inwiefern die in den Leitlinien, Normen und anderen anwendbaren Vorschriften festgelegten Informationssicherheitsanforderungen eingehalten werden. Die automatischen Bemessungs- und Berichterstattungstools sollten bei einer effizienten, regelmäßigen Prüfung berücksichtigt werden.

Falls bei der Prüfung ein Konformitätsverstoß festgestellt wird, sollten die Manager die folgenden Maßnahmen ergreifen:

a) Feststellung der Ursachen des Konformitätsverstoßes;

b) Beurteilung, ob Maßnahmen zur Herstellung der Konformität erforderlich sind;

c) Umsetzung geeigneter Korrekturmaßnahmen;

d) Prüfung der unternommenen Korrekturmaßnahmen, um deren Wirksamkeit zu verifizieren und jedwede Defizite oder Schwachstellen festzustellen.

Die Ergebnisse der von den Managern durchgeführten Prüfungen und Korrekturmaßnahmen sollten aufgezeichnet und die Aufzeichnungen sollten aufbewahrt werden. Das Management sollte die Ergebnisse an die Personen berichten, die die unabhängigen Prüfungen durchführen (siehe 18.2.1), wenn in ihrem Verantwortungsbereich eine unabhängige Prüfung stattfindet.

Weitere Informationen

Die betriebliche Überwachung der Systemnutzung wird in 12.4 behandelt.

18.2.3 Technische Konformitätsprüfung

Maßnahme

Informationssysteme sollten regelmäßig auf Konformität mit den Informationssicherheitsleitlinien und -normen der Organisation geprüft werden.

Umsetzungshinweise

Die technische Konformität sollte bevorzugt mit Hilfe automatischer Tools geprüft werden, mit denen technische Berichte erzeugt werden, die anschließend von einem technischen Experten interpretiert werden. Alternativ könnten manuelle Prüfungen (ggf. mit Unterstützung entsprechender Software-Tools) von einem erfahrenen Systemingenieur durchgeführt werden.

Falls Penetrationstests oder Schwachstellenuntersuchungen vorgenommen werden, sollte besondere Vorsicht geübt werden, da derartige Aktivitäten zu einer Kompromittierung der Systemsicherheit führen können. Derartige Tests sollten geplant und dokumentiert werden sowie wiederholbar sein.

Eine technische Konformitätsprüfung sollte nur von kompetenten, autorisierten Personen oder unter deren Aufsicht durchgeführt werden.

Weitere Informationen

Technische Konformitätsprüfungen beinhalten die Untersuchung der betrieblichen Systeme, um sicherzustellen, dass die hardware- und softwarebezogenen Kontrollmaßnahmen ordnungsnach implementiert wurden. Eine Konformitätsprüfung dieser Art erfordert spezialisierte technische Fachkompetenzen.

Die Konformitätsprüfungen umfassen z. B. auch Penetrationstests und Schwachstellenuntersuchungen, die von unabhängigen, eigens damit beauftragten Experten durchgeführt werden können. Dies kann hilfreich zur Erkennung von Schwachstellen im System sein sowie zur Überprüfung der Wirksamkeit der Maßnahmen zur Verhinderung eines diese Schwachstellen ausnutzenden, nicht autorisierten Zugriffs.

Penetrationstests und Schwachstellenuntersuchungen bieten die Momentaufnahme eines Systems in einem bestimmten Zustand zu einem bestimmten Zeitpunkt. Diese Momentaufnahme beschränkt sich auf jene Bereiche des Systems, in denen die Penetrationsversuche stattgefunden haben. Penetrationstests und Schwachstellenuntersuchungen sind zur Risikoeinschätzung nicht geeignet.

ISO/IEC TR 27008 enthält spezifische Anleitungen zur Durchführung von technischen Konformitätsprüfungen.

Literaturhinweise

[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*

[2] ISO/IEC 11770, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770, *Information technology Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770, *Information technology Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 2000-1:2012 *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2:2005 *Information technology — Service management — Part 2: Code of practice*

[8] ISO/IEC 22301, *Societal security — Business continuity management systems — Requirements*

[9] ISO/IEC 22313:2012, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033, *Information technology — Security techniques — Network security — Part* 1: Overview and concepts

[16] ISO/IEC 27033, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[18] *ISO/IEC 27033, Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

[22] ISO/IEC 27036, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*

[23] ISO/IEC 27036, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and guidelines*