

DIN EN ISO/IEC 27002

ICS 35.030

Entwurf

Einsprüche bis 2022-09-15
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27002:2017-06

**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022);
Deutsche und Englische Fassung prEN ISO/IEC 27002:2022**

Information security, cybersecurity and privacy protection –
Information security controls (ISO/IEC 27002:2022);
German and English version prEN ISO/IEC 27002:2022

Sécurité de l'information, cybersécurité et protection de la vie privée –
Mesures de sécurité de l'information (ISO/IEC 27002:2022);
Version allemande et anglaise prEN ISO/IEC 27002:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-07-15 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe 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/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin oder Am DIN-Platz, 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 368 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)



Nationales Vorwort

Der Text von ISO/IEC 27002:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27702:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 9000	siehe	DIN EN ISO 9000
ISO 55001	siehe	DIN ISO 55001
ISO 22301	siehe	DIN EN ISO 22301
ISO 22313	siehe	DIN EN ISO 22313
ISO 27799	siehe	DIN EN ISO 27799
ISO 31000:2018	siehe	DIN ISO 31000:2018-10
ISO/IEC 15408 (alle Teile)	siehe	DIN EN ISO/IEC 15408-1
		DIN EN ISO/IEC 15408-2
		DIN EN ISO/IEC 15408-3
ISO/IEC 17788	siehe	DIN ISO/IEC 17788
ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO/IEC 19086 (alle Teile)	siehe	DIN ISO/IEC 19086-1
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27011	siehe	DIN EN ISO/IEC 27011
ISO/IEC 27017	siehe	DIN EN ISO/IEC 27017
ISO/IEC 27018	siehe	DIN EN ISO/IEC 27018
ISO/IEC 27019	siehe	DIN EN ISO/IEC 27019
ISO/IEC 27037	siehe	DIN EN ISO/IEC 27037
ISO/IEC 27040	siehe	DIN EN ISO/IEC 27040
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29134	siehe	DIN EN ISO/IEC 29134
ISO/IEC 29147	siehe	DIN EN ISO/IEC 29147
ISO/IEC 30111	siehe	DIN EN ISO/IEC 30111

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO/IEC 27002:2017-06 wurden folgende Änderungen vorgenommen:

- a) der Titel wurde geändert;
- b) die Struktur des Dokuments wurde geändert, die Maßnahmen werden nun mit einer einfachen Taxonomie und den zugehörigen Attributen dargestellt;
- c) einige Maßnahmen wurden zusammengelegt, einige wurden gelöscht und mehrere neue Maßnahmen wurden eingeführt. Die Zusammenhänge werden in Anhang B dargestellt;
- d) redaktionelle Überarbeitung der Norm.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9000, *Qualitätsmanagementsysteme — Grundlagen und Begriffe*

DIN EN ISO 22301, *Sicherheit und Resilienz — Business Continuity Management System — Anforderungen*

DIN EN ISO 22313, *Sicherheit und Resilienz — Business Continuity Management System — Anleitung zur Verwendung von ISO 22301*

DIN EN ISO 27799, *Medizinische Informatik — Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002*

DIN EN ISO/IEC 15408-1, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell*

DIN EN ISO/IEC 15408-2, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten*

DIN EN ISO/IEC 15408-3, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3: Komponenten zur Sicherheitskontrolle*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27011, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen*

DIN EN ISO/IEC 27017, *Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste*

DIN EN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

DIN EN ISO/IEC 27019, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmaßnahmen für die Energieversorgung*

DIN EN ISO/IEC 27037, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel*

DIN EN ISO/IEC 27040, *Informationstechnik — IT-Sicherheitsverfahren — Speichersicherheit*

DIN EN ISO/IEC 27701, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

DIN EN ISO/IEC 29134, *Informationstechnik — Sicherheitsverfahren — Leitlinien für die Datenschutz-Folgenabschätzung*

DIN EN ISO/IEC 29147, *Informationstechnik — Sicherheitstechniken — Offenlegung von Schwachstellen*

DIN EN ISO/IEC 30111, *Informationstechnik — IT-Sicherheitsverfahren — Prozesse für die Behandlung von Schwachstellen*

DIN ISO 55001, *Asset Management — Managementsysteme — Anforderungen*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

DIN ISO/IEC 17788, *Informationstechnik — Cloud Computing — Übersicht und Vokabular*

DIN ISO/IEC 17789, *Informationstechnik — Cloud Computing — Referenzarchitektur*

DIN ISO/IEC 19086-1, *Informationstechnik — Cloud Computing — Dienstgütevereinbarung (SLA) Rahmenwerk — Teil 1: Übersicht und Konzepte*

<i>Titel de:</i>	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)
<i>Titel en:</i>	Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC 27002:2022)
<i>Titel fr:</i>	Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information (ISO/IEC 27002:2022)

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	8
1 Anwendungsbereich	11
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	11
3.1 Begriffe	11
3.2 Abkürzungen	17
4 Aufbau dieses Dokuments	18
4.1 Abschnitte	18
4.2 Themen und Attribute	19
4.3 Maßnahmengestaltung	20
5 Organisatorische Maßnahmen	21
5.1 Informationssicherheitsrichtlinien	21
5.2 Informationssicherheitsrollen und -verantwortlichkeiten	23
5.3 Aufgabentrennung	24
5.4 Verantwortlichkeiten der Leitung	26
5.5 Kontakt mit Behörden	27
5.6 Kontakt mit speziellen Interessensgruppen	28
5.7 Bedrohungsentelligenz	28
5.8 Informationssicherheit im Projektmanagement	30
5.9 Inventar der Informationen und anderen damit verbundenen Werten	32
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	34
5.11 Rückgabe von Werten	36
5.12 Klassifizierung von Information	37
5.13 Kennzeichnung von Information	39
5.14 Informationsübertragung	40
5.15 Zugangssteuerung	43
5.16 Identitätsmanagement	46
5.17 Informationen zur Authentifizierung	47
5.18 Zugangsrechte	50
5.19 Informationssicherheit in Lieferantenbeziehungen	52
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	54
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	57
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	59
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten	61
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	64
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse	66
5.26 Reaktion auf Informationssicherheitsvorfälle	67
5.27 Erkenntnisse aus Informationssicherheitsvorfällen	68
5.28 Sammeln von Beweismaterial	69
5.29 Informationssicherheit bei Störungen	70
5.30 IKT-Bereitschaft für Business Continuity	71
5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	72

5.32	Geistige Eigentumsrechte.....	74
5.33	Schutz von Aufzeichnungen.....	76
5.34	Datenschutz und Schutz personenbezogener Daten (pbD).....	78
5.35	Unabhängige Überprüfung der Informationssicherheit.....	79
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit.....	80
5.37	Dokumentierte Betriebsabläufe.....	81
6	Personenbezogene Maßnahmen.....	83
6.1	Sicherheitsüberprüfung.....	83
6.2	Beschäftigungs- und Vertragsbedingungen.....	84
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	86
6.4	Maßregelungsprozess.....	88
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung.....	89
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	90
6.7	Telearbeit.....	91
6.8	Meldung von Informationssicherheitsereignissen.....	93
7	Physische Maßnahmen.....	94
7.1	Physische Sicherheitsperimeter.....	94
7.2	Physischer Zutritt.....	95
7.3	Sichern von Büros, Räumen und Einrichtungen.....	97
7.4	Physische Sicherheitsüberwachung.....	98
7.5	Schutz vor physischen und umweltbedingten Bedrohungen.....	99
7.6	Arbeiten in Sicherheitsbereichen.....	101
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	102
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln.....	103
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten.....	104
7.10	Speichermedien.....	105
7.11	Versorgungseinrichtungen.....	107
7.12	Sicherheit der Verkabelung.....	108
7.13	Instandhaltung von Geräten und Betriebsmitteln.....	109
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln.....	110
8	Technologische Maßnahmen.....	112
8.1	Endpunktgeräte des Benutzers.....	112
8.2	Privilegierte Zugangsrechte.....	114
8.3	Informationszugangsbeschränkung.....	116
8.4	Zugriff auf den Quellcode.....	118
8.5	Sichere Authentifizierung.....	119
8.6	Kapazitätssteuerung.....	121
8.7	Schutz gegen Schadsoftware.....	123
8.8	Handhabung von technischen Schwachstellen.....	125
8.9	Konfigurationsmanagement.....	129
8.10	Löschung von Informationen.....	131
8.11	Datenmaskierung.....	133
8.12	Verhinderung von Datenlecks.....	135
8.13	Sicherung von Information.....	136
8.14	Redundanz von informationsverarbeitenden Einrichtungen.....	138
8.15	Protokollierung.....	139
8.16	Überwachung von Aktivitäten.....	142
8.17	Uhrensynchronisation.....	145
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten.....	146
8.19	Installation von Software auf Systemen im Betrieb.....	147
8.20	Netzwerksicherheit.....	148
8.21	Sicherheit von Netzwerkdiensten.....	150
8.22	Trennung von Netzwerken.....	151
8.23	Webfilterung.....	152

8.24	Verwendung von Kryptographie.....	153
8.25	Lebenszyklus einer sicheren Entwicklung.....	156
8.26	Anforderungen an die Anwendungssicherheit.....	157
8.27	Sichere Systemarchitektur und technische Grundsätze	160
8.28	Sicheres Coding	162
8.29	Sicherheitsprüfung in Entwicklung und Abnahme	165
8.30	Ausgegliederte Entwicklung.....	167
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	168
8.32	Änderungssteuerung.....	170
8.33	Prüfinformationen	171
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	172
Anhang A (informativ) Verwendung von Attributen.....		174
A.1	Allgemeines	174
A.2	Organisatorische Sichten.....	192
Anhang B (informativ) Übereinstimmung von ISO/IEC 27002:2022 (dieses Dokument) mit ISO/IEC 27002:2013		194
Literaturhinweise.....		202

Europäisches Vorwort

Der Text von ISO/IEC 27002:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27702:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27002:2022 wurde von CEN als prEN ISO/IEC 27002:2022 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder der IEC-Liste der erhaltenen Patenterklärungen (siehe patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe <https://www.iec.ch/understanding-standards>.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27002:2013), die technisch überarbeitet wurde. Sie berücksichtigt auch die Berichtigungen ISO/IEC 27002:2013/Cor. 1:2014 und ISO/IEC 27002:2013/Cor. 2:2015.

Die wesentlichen Änderungen sind Folgende:

- der Titel wurde modifiziert;
- die Struktur des Dokuments wurde geändert, indem die Maßnahmen mit einer einfachen Taxonomie und zugehörigen Attributen dargestellt werden;
- einige Maßnahmen wurden zusammengelegt, einige gestrichen und mehrere neue Maßnahmen wurden eingeführt. Die vollständige Übereinstimmung kann Anhang B entnommen werden.

Diese korrigierte Version der ISO/IEC 27002:2022 enthält die folgenden Korrekturen:

- nicht funktionierende Hyperlinks im gesamten Dokument wurden wiederhergestellt;
- in der einleitenden Tabelle in Unterabschnitt 5.22 und in Tabelle A.1 (Zeile 5.22) wurde „#Information_Sicherheit_Vertrauenswürdigkeit“ von der Spalte „Sicherheitsdomänen“ in die Spalte „Betriebsfähigkeit“ verschoben.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und <https://www.iec.ch/national-committees> zu finden.

Einleitung

0.1 Hintergrund und Kontext

Dieses Dokument wurde für Organisationen jeder Art und Größe erarbeitet. Es soll als Referenz für die Bestimmung und Implementierung von Maßnahmen zur Behandlung von Informationssicherheitsrisiken in einem Managementsystem für Informationssicherheit (ISMS) auf der Grundlage von ISO/IEC 27001 verwendet werden. Es kann auch als Leitfaden für Organisationen verwendet werden, die allgemein anerkannte Informationssicherheitsmaßnahmen festlegen und umsetzen. Darüber hinaus ist dieses Dokument ebenfalls bestimmt für die Entwicklung von branchen- und organisationsspezifischen Leitlinien zum Management von Informationssicherheit, die deren spezifisches Umfeld der Informationssicherheitsrisiken berücksichtigen. Organisatorische oder umgebungsspezifische Maßnahmen, die nicht in diesem Dokument enthalten sind, können bei Bedarf durch eine Risikobeurteilung festgelegt werden.

Organisationen aller Arten und Größen (einschließlich öffentlicher und privater, kommerzieller und gemeinnütziger) erheben, verarbeiten, speichern übertragen und vernichten 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. In einer vernetzten Welt verdienen oder erfordern Informationen und andere damit verbundene Werte Schutz vor verschiedenen Risikoquellen, seien sie natürlich, zufällig oder vorsätzlich.

Die Einführung einer Reihe geeigneter Sicherheitsmaßnahmen, darunter Richtlinien, Regeln, Prozesse, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen, sorgt für Informationssicherheit. Um ihre spezifischen Sicherheits- und Geschäftsziele zu erreichen, sollte die Organisation diese Maßnahmen festlegen, umsetzen, überwachen, überprüfen und gegebenenfalls verbessern. Ein Informationssicherheitsmanagementsystem (ISMS), wie in ISO/IEC 27001 näher beschrieben, verfolgt eine ganzheitliche, koordinierte Betrachtung der Risiken in der Informationssicherheit einer Organisation, um eine umfassende Sammlung von Maßnahmen zur Informationssicherheit innerhalb eines einheitlichen Managementsystems bestimmen und einführen zu können.

Viele Informationssysteme, einschließlich deren Management und Betrieb, sind nicht so konzipiert, dass sie im Sinne eines ISMS, wie es in ISO/IEC 27001 und diesem Dokument beschrieben ist, als sicher betrachtet werden können. Die Sicherheitsstufe, die allein durch technische Maßnahmen erreicht werden kann, ist begrenzt und sollte durch geeignete Managementaktivitäten und organisatorische Prozesse unterstützt werden. Die Feststellung der benötigten Sicherheitsmaßnahmen erfordert sorgfältige Planung und Detailtreue bei der Risikobehandlung.

Ein erfolgreiches Informationssicherheitsmanagementsystem erfordert die Mitarbeit des gesamten Personals einer Organisation. Sie kann auch die Beteiligung anderer interessierter Parteien, wie z. B. Aktionäre oder Lieferanten, erfordern. Auch der Rat von Fachleuten kann erforderlich sein.

Ein geeignetes, angemessenes und wirksames Managementsystem für die Informationssicherheit bietet der Leitung der Organisation und anderen interessierten Parteien die Vertrauenswürdigkeit, dass ihre Informationen und andere damit verbundenen Werte angemessen sicher und vor Bedrohungen und Schäden geschützt sind, so dass die Organisation ihre erklärten Geschäftsziele erreichen kann.

0.2 Anforderungen an Informationssicherheit

Es ist wichtig, dass eine Organisation ihre Anforderungen an die Informationssicherheit festlegt. Es existieren drei Hauptquellen für Anforderungen an die Informationssicherheit:

- a) die Beurteilung von Risiken für die Organisation unter Berücksichtigung der Unternehmensstrategie und der Geschäftsziele. Dies kann durch eine informationssicherheitsspezifische Risikobeurteilung erleichtert oder unterstützt werden. Dies sollte zur Bestimmung der Maßnahmen führen, die erforderlich sind, um sicherzustellen, dass das Restrisiko für die Organisation die Risikoannahmekriterien erfüllt;
- b) die rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen, die eine Organisation und ihre interessierten Parteien (Handelspartner, Dienstleister usw.) zu erfüllen haben, sowie ihr soziokulturelles Umfeld;
- c) eine Reihe von Grundsätzen, Zielen und Geschäftsanforderungen, die eine Organisation für alle Schritte des Lebenszyklus von Informationen, die eine Organisation zur Unterstützung ihrer Geschäftstätigkeit entwickelt hat.

0.3 Maßnahmen

Eine Kontrollmaßnahme, die das Risiko verändert oder aufrechterhält, wird als Maßnahme definiert. Einige der Maßnahmen in diesem Dokument verändern das Risiko, während andere das Risiko aufrechterhalten. Eine Informationssicherheitsrichtlinie kann zum Beispiel das Risiko nur aufrechterhalten, während die Einhaltung der Informationssicherheitsrichtlinie das Risiko verändern kann. Außerdem beschreiben einige Kontrollmaßnahmen dieselbe generische Maßnahme in unterschiedlichen Risikokontexten. Dieses Dokument bietet eine generische Mischung aus organisatorischen, personellen, physischen und technologischen Informationssicherheitsmaßnahmen, die von international anerkannten bewährten Verfahren abgeleitet sind.

0.4 Bestimmen derzeitiger Maßnahmen

Die Festlegung von Maßnahmen hängt von den Entscheidungen der Organisation im Anschluss an eine Risikobeurteilung mit einem klar definierten Anwendungsbereich ab. Entscheidungen in Bezug auf festgestellte Risiken sollten auf den Kriterien für die Annahme des Risikos, den Optionen für die Risikobehandlung und dem durch die Organisation angewendeten Ansatz für das Risikomanagement beruhen. Bei der Festlegung der Maßnahmen sollten auch alle einschlägigen nationalen und internationalen Gesetze und Vorschriften berücksichtigt werden. Die Festlegung der Maßnahmen hängt ebenfalls von der Art und Weise ab, wie Maßnahmen miteinander interagieren, um gestaffelte Sicherheitsebenen bereitstellen zu können.

Die Organisation kann Maßnahmen nach Bedarf gestalten oder aus einer beliebigen Quelle auswählen. Bei der Festlegung solcher Maßnahmen sollte die Organisation die Ressourcen und Investitionen, die für die Implementierung und den Betrieb einer Maßnahme erforderlich sind, gegen den erzielten Geschäftswert abwägen. Siehe ISO/IEC TR 27016 als Leitfaden für Entscheidungen über die Investition in ein ISMS und die wirtschaftlichen Folgen dieser Entscheidungen im Zusammenhang mit konkurrierenden Anforderungen an Ressourcen.

Es sollte ein ausgewogenes Verhältnis zwischen den für die Durchführung von Maßnahmen eingesetzten Ressourcen und den potentiellen Auswirkungen von Sicherheitsvorfällen auf das Unternehmen bei Fehlen dieser Maßnahmen bestehen. Die Ergebnisse einer Risikobeurteilung sollten dabei helfen, geeignete betriebliche Maßnahmen, Prioritäten zur Bewältigung von Risiken der Informationssicherheit und für die Umsetzung von Maßnahmen, die zum Schutz vor diesen Risiken erforderlich sind, zu bestimmen.

Einige der Maßnahmen in diesem Dokument können als Leitlinien für das Management der Informationssicherheit betrachtet werden und sind in den meisten Organisationen anwendbar. Weitere Informationen zur Bestimmung von Maßnahmen und anderen Risikobehandlungsmöglichkeiten sind in ISO/IEC 27005 verfügbar.

0.5 Entwicklung organisationsspezifischer Leitlinien

Dieses Dokument kann als Ausgangspunkt für die Entwicklung organisationsspezifischer Leitlinien angesehen werden. Nicht alle Maßnahmen und Anleitungen in diesem Dokument lassen sich auf alle Organisationen anwenden. Zusätzliche Maßnahmen und Leitlinien, die nicht in diesem Dokument enthalten sind, können ebenfalls erforderlich sein, um den spezifischen Bedürfnissen der Organisation und den ermittelten Risiken gerecht zu werden. Bei der Ausarbeitung von Dokumenten, die weitere Leitfäden oder Maßnahmen enthalten, kann die Aufnahme von Verweisungen auf Abschnitte des vorliegenden Dokuments von Nutzen sein, um später darauf verweisen zu können.

0.6 Überlegungen zum Lebenszyklus

Informationen haben einen Lebenszyklus, von der Erstellung bis zur Entsorgung. Der Wert von Informationen und die Risiken für diese können während des gesamten Lebenszyklus variieren (z. B. ist die unbefugte Offenlegung oder der Diebstahl des Geschäftsberichts eines Unternehmens nach dessen Veröffentlichung nicht mehr von Bedeutung, aber die Integrität bleibt kritisch), weshalb die Informationssicherheit in allen Phasen in gewissem Maß von Wichtigkeit ist.

Informationssysteme und andere für die Informationssicherheit relevante Vermögenswerte unterliegen Lebenszyklen, in denen sie konzipiert, festgelegt, entworfen, entwickelt, geprüft, umgesetzt, genutzt, gepflegt und schließlich ausgemustert und entsorgt werden. Informationssicherheit sollte in jeder Phase berücksichtigt werden. Neue Systementwicklungsprojekte und Änderungen an bestehenden Systemen bieten die Möglichkeit, die Sicherheitsmaßnahmen zu verbessern und dabei die Risiken des Unternehmens und die aus Vorfällen gewonnenen Erkenntnisse zu berücksichtigen.

0.7 Zugehörige internationale Normen

Während dieses Dokument als Orientierung für ein breites Spektrum an Maßnahmen für Informationssicherheit anzusehen ist, die üblicherweise in vielen Organisationen angewendet werden, bieten andere Dokumente in der ISO/IEC 27000-Familie 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 Dokumentenfamilie. ISO/IEC 27000 enthält ein Glossar für Definitionen der meisten Begriffe, die in der ISO/IEC 27000-Dokumentenfamilie verwendet werden, und beschreibt den Anwendungsbereich und die Ziele einzelner Normen.

Es gibt sektorspezifische Normen mit zusätzlichen Maßnahmen, die auf bestimmte Bereiche abzielen (z. B. ISO/IEC 27017 für Cloud-Dienste, ISO/IEC 27701 für Datenschutz, ISO/IEC 27019 für Energie, ISO/IEC 27011 für Telekommunikationsunternehmen und ISO 27799 für Gesundheit). Diese Normen sind in den Literaturhinweisen aufgeführt, und auf einige von ihnen wird in den Abschnitten „Leitfaden“ und „Sonstige Informationen“ in Abschnitt 5 bis Abschnitt 8 verwiesen.

1 Anwendungsbereich

Dieses Dokument enthält einen Referenzsatz allgemeiner Informationssicherheitsmaßnahmen einschließlich einem Leitfaden zur Umsetzung. Dieses Dokument wurde für Organisationen entwickelt:

- a) im Rahmen eines Managementsystems für Informationssicherheit (ISMS) auf der Basis von ISO/IEC 27001;
- b) für die Umsetzung von Maßnahmen zur Informationssicherheit auf der Grundlage international anerkannter bewährter Verfahren;
- c) zur Entwicklung organisationsspezifischer Leitfäden für das Management der Informationssicherheit.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1.1

Zugangssteuerung

Mittel, um sicherzustellen, dass der physische und logische Zugang zu *Werten* (3.1.2) aufgrund von Geschäfts- und Informationssicherheitsanforderungen befugt und eingeschränkt ist

3.1.2

Wert

alles, was für die Organisation von Bedeutung und/oder von Nutzen ist

Anmerkung 1 zum Begriff: Im Zusammenhang mit der Informationssicherheit können zwei Arten von Werten unterschieden werden:

- die Primärwerte:
 - Informationen;
 - Geschäftsprozesse (3.1.27) und -aktivitäten;
- die unterstützenden Werte (von denen die Primärwerte abhängen) aller Art, zum Beispiel:
 - Hardware;
 - Software;
 - Netzwerk;
 - *Personal* (3.1.20);
 - Standort;
 - Struktur der Organisation.

3.1.3

Angriff

erfolgreicher oder erfolgloser unbefugter Versuch, einen Wert zu zerstören, zu verändern, unbrauchbar zu machen, sich Zugang zu einem *Wert* (3.1.2) zu verschaffen oder jeder Versuch, einen *Wert* (3.1.2) preiszugeben, zu stehlen oder unbefugt zu nutzen

3.1.4

Authentisierung

Sicherstellung, dass die von einer *Entität* (3.1.11) behaupteten Eigenschaften richtig sind

3.1.5

Authentizität

Eigenschaft, dass eine *Entität* (3.1.11) das ist, was sie angibt zu sein

3.1.6

Kontrollkette

nachweislicher Besitz, Bewegung, Handhabung und Verbleib von Material von einem Zeitpunkt bis zu einem anderen

Anmerkung 1 zum Begriff: Das Material umfasst Informationen und andere zugehörige *Werte* (3.1.2) im Rahmen von ISO/IEC 27002.

[QUELLE: ISO/IEC 27050-1:2019, 3.1, modifiziert — Anmerkung 1 zum Begriff hinzugefügt.]

3.1.7

vertrauliche Informationen

Informationen, die nicht dazu bestimmt sind, unbefugten Personen, *Entitäten* (3.1.11) oder *Prozessen* (3.1.27) zugänglich gemacht oder offengelegt zu werden

3.1.8

Steuerung

Maßnahme, die das Risiko beibehält und/oder verändert

Anmerkung 1 zum Begriff: Steuerungen umfassen unter anderem alle *Prozesse* (3.1.27), *Politik* (3.1.24), Instrumente, Verfahren oder andere Bedingungen und/oder Aktionen, welche Risiken beibehalten oder verändern.

Anmerkung 2 zum Begriff: Steuerungen können nicht immer die beabsichtigte oder angenommene verändernde Wirkung ausüben.

[QUELLE: ISO 31000:2018, 3.8]

3.1.9

Störung

Zwischenfall, ob vorhergesehen oder unvorhergesehen, der entsprechend den Zielsetzungen einer Organisation eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen verursacht

[QUELLE: ISO 22301:2019, 3.10]

3.1.10

Endpunktgerät

netzwerkgebundenes Hardware-Gerät der Informations- und Kommunikationstechnologie (IKT)

Anmerkung 1 zum Begriff: Endpunktgeräte können sich auf Desktop-Computer, Laptops, Smartphones, Tablets, Thin-Clients, Drucker oder andere Spezialhardware wie intelligente Zähler und IoT-Geräte (Internet der Dinge, en: Internet of Things) beziehen.

3.1.11

Entität

Begriff, der für den Betrieb einer Domäne relevant ist und erkennbar eine eigene Existenz hat

Anmerkung 1 zum Begriff: Eine Entität kann eine physische oder eine logische Ausführungsform haben.

BEISPIEL Eine Person, eine Organisation, ein Gerät, eine Gruppe solcher Begriffe, ein menschlicher Teilnehmer an einem Telekommunikationsdienst, eine SIM-Karte, ein Reisepass, eine Netzwerkkarte, eine Softwareanwendung, ein Dienst oder eine Website.

[QUELLE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12

informationsverarbeitende Einrichtung

jedes informationsverarbeitende System, jeder informationsverarbeitende Dienst oder jede informationsverarbeitende Infrastruktur oder der physische Standort, der diese beherbergt

[QUELLE: ISO/IEC 27000:2018, 3.27, modifiziert — „Einrichtungen“ wurde durch „Einrichtung“ ersetzt.]

3.1.13

Informationssicherheitsverletzung

Beeinträchtigung der Informationssicherheit, die zur unerwünschten Zerstörung, zum Verlust, zur Veränderung, zur Offenlegung von oder zum Zugriff auf geschützte Informationen bei deren Übertragung, Speicherung oder sonstiger Verarbeitung führt

3.1.14

Informationssicherheitsereignis

Vorkommnisse, die auf eine mögliche *Verletzung der Informationssicherheit* (3.1.13) oder ein Versagen der *Maßnahmen* (3.1.8) hinweisen

[QUELLE: ISO/IEC 27035-1:2016, 3.3, modifiziert — „Verletzung der Informationssicherheit“ wurde durch „Informationssicherheitsverletzung“ ersetzt.]

3.1.15

Informationssicherheitsvorfall

ein oder mehrere zusammenhängende und identifizierte *Informationssicherheitsereignisse* (3.1.14), die den *Werten* (3.1.2) einer Organisation schaden oder ihren Betrieb gefährden können

[QUELLE: ISO/IEC 27035-1:2016, 3.4]

3.1.16

Handhabung von Informationssicherheitsvorfällen

Ausübung einer konsistenten und wirksamen Herangehensweise für die Handhabung von *Informationssicherheitsvorfällen* (3.1.15)

[QUELLE: ISO/IEC 27035-1:2016, 3.5]

3.1.17

Informationssystem

Anwendungen, Dienste, informationstechnische *Werte* (3.1.2) oder andere Information bearbeitende Komponenten

[QUELLE: ISO/IEC 27000:2018, 3.35]

3.1.18

interessierte Partei

Anspruchsgruppe

Person oder Organisation, die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann

[QUELLE: ISO/IEC 27000:2018, 3.37]

3.1.19

Nichtabstreitbarkeit

Fähigkeit, das Eintreten eines behaupteten Ereignisses oder einer behaupteten Handlung samt ihren ursächlichen *Entitäten* (3.1.11) nachzuweisen

3.1.20

Personal

Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten

Anmerkung 1 zum Begriff: Der Begriff „Personal“ umfasst die Mitglieder der Organisation, z. B. das Steuerungsgremium, die oberste Leitung, die Beschäftigten, die Zeitarbeiter, die Auftragnehmer und die Freiwilligen.

3.1.21

personenbezogene Daten

pbD

alle Daten bzw. Informationen, die (a) dazu verwendet werden können, eine Verbindung zwischen ihnen und der natürlichen Person, auf die sie sich beziehen, herzustellen, oder (b) direkt oder indirekt mit einer natürlichen Person verknüpft sind oder verknüpft werden können

Anmerkung 1 zum Begriff: Die „natürliche Person“ in der Definition entspricht dem/der *Betroffenen* (3.1.22). Um festzustellen, ob ein/e Betroffene/r identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von Betroffenen, Verantwortlichen oder anderen Interessengruppen des Datenschutzes, die im Besitz der Daten sind, oder von einer beliebigen anderen Partei angewendet werden können, um eine Verbindung zwischen den pbD und der natürlichen Person herzustellen.

[QUELLE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22

Betroffene/r

natürliche Person, auf die sich die *personenbezogenen Daten* (pbD) (3.1.21) beziehen

Anmerkung 1 zum Begriff: Abhängig von der Rechtsprechung und der jeweiligen Gesetzgebung zum Datenschutz und zum Schutz personenbezogener Daten kann anstelle der Benennung „Betroffener/Betroffene (en: PII principal)“ auch das Synonym „Datensubjekt (en: data subject)“ verwendet werden.

[QUELLE: ISO/IEC 29100:2011, 2.11]

3.1.23

Auftragsdatenverarbeiter

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die *personenbezogene Daten* (pbD) (3.1.21) im Namen und nach den Anweisungen einer verantwortlichen Stelle verarbeiten

[QUELLE: ISO/IEC 29100:2011, 2.12]

3.1.24

Politik

Absichten und Ausrichtung einer Organisation, wie von der obersten Leitung formell ausgedrückt

[QUELLE: ISO/IEC 27000:2018, 3.53]

3.1.25

Datenschutz-Folgenabschätzung

DSFA

Gesamtprozess (3.1.27) aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung *personenbezogener Daten* (*pbD*) (3.1.21), eingebettet in den unternehmensweiten Rahmen zum Risikomanagement

[QUELLE: ISO/IEC 29134:2017, 3.7, modifiziert – Anmerkung 1 zum Begriff entfernt.]

3.1.26

Verfahren

festgelegte Art und Weise, eine Tätigkeit oder einen *Prozess* (3.1.27) auszuführen

[QUELLE: ISO 30000:2009, 3.12]

3.1.27

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben verwendet oder umwandelt, um ein Ergebnis bereitzustellen

[QUELLE: ISO 9000:2015, 3.4.1, modifiziert – Anmerkungen zum Begriff entfernt.]

3.1.28

Aufzeichnung

Informationen, die von einer Organisation oder Person in Erfüllung rechtlicher Verpflichtungen oder im Rahmen der Geschäftsabwicklung als Beweismittel und als *Wert* (3.1.2) erstellt, erhalten und aufbewahrt werden

Anmerkung 1 zum Begriff: Rechtliche Verpflichtungen umfassen in diesem Zusammenhang alle rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen.

[QUELLE: ISO 15489-1:2016, 3.14, modifiziert – Anmerkung 1 zum Begriff hinzugefügt.]

3.1.29

Wiederherstellungspunkt

RPO, en: recovery point objective

Zeitpunkt, bis zu dem die Daten nach einer *Störung* (3.1.9) wiederherzustellen sind

[QUELLE: ISO/IEC 27031:2011, 3.12, modifiziert – „müssen“ ersetzt durch „sind zu“.]

3.1.30

Wiederherstellungsdauer

RTO, en: recovery time objective

Zeitspanne, innerhalb derer ein Mindestmaß an Diensten und/oder Produkten sowie die unterstützenden Systeme, Anwendungen oder Funktionen nach einer *Störung* (3.1.9) wiederherzustellen sind

[QUELLE: ISO/IEC 27031:2011, 3.13, modifiziert – „müssen“ ersetzt durch „sind zu“.]

3.1.31

Zuverlässigkeit

Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen

3.1.32

Regel

anerkannter Grundsatz oder Anweisung, der/die die Erwartungen der Organisation in Bezug auf das, was getan werden muss, erlaubt oder nicht erlaubt ist, festlegt

Anmerkung 1 zum Begriff: Regeln können in *themenspezifischen Richtlinien* (3.1.35) und in anderen Arten von Dokumenten formell ausgedrückt werden.

3.1.33

sensible Informationen

Informationen, die vor Nichtverfügbarkeit, unbefugtem Zugriff, Veränderung oder öffentlicher Bekanntgabe geschützt werden müssen, weil sie potentiell nachteilige Auswirkungen auf eine Person, eine Organisation, die nationale Sicherheit oder den Schutz der Öffentlichkeit haben könnten

3.1.34

Bedrohung

mögliche Ursache eines unerwünschten Vorfalles, der zu Schaden für ein System oder eine Organisation führen kann

[QUELLE: ISO/IEC 27000:2018, 3.74]

3.1.35

themenspezifische Richtlinie

Absichten und Ausrichtung zu einem bestimmten Subjekt oder Thema, wie sie von der zuständigen Managementebene formell zum Ausdruck gebracht wurden

Anmerkung 1 zum Begriff: Themenspezifische Richtlinien können formell *Regeln* (3.1.32) oder Organisationsnormen ausdrücken.

Anmerkung 2 zum Begriff: Einige Organisationen verwenden andere Ausdrücke für diese themenspezifischen Richtlinien.

Anmerkung 3 zum Begriff: Die themenspezifischen Richtlinien, auf die in diesem Dokument Bezug genommen wird, beziehen sich auf die Informationssicherheit.

BEISPIEL Themenspezifische Richtlinie über die *Zugangssteuerung* (3.1.1), themenspezifische Richtlinie über eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.

3.1.36

Benutzer

interessierte Partei (3.1.18) mit Zugang zu den *Informationssystemen* (3.1.17) der Organisation

BEISPIEL *Personal* (3.1.20), Kunden, Lieferanten.

3.1.37

Endpunktgerät des Benutzers

Endpunktgerät (3.1.10), das von Benutzern für den Zugriff auf Informationsverarbeitungsdienste verwendet wird

Anmerkung 1 zum Begriff: Endpunktgeräte des Benutzers können sich auf Desktop-Computer, Laptops, Smartphones, Tablets, Thin-Clients usw. beziehen.

3.1.38

Schwachstelle

Schwäche eines *Wertes* (3.1.2) oder einer *Maßnahme* (3.1.8), die durch eine oder mehrere *Bedrohungen* (3.1.34) ausgenutzt werden kann

[QUELLE: ISO/IEC 27000:2018, 3.77]

3.2 Abkürzungen

ABAC	attributbasierte Zugangssteuerung (en: attribute-based access control)
ACL	Zugriffskontrollliste (en: access control list)
BIA	Business-Impact-Analyse
BYOD	Bring Your Own Device
CAPTCHA	Vollständig automatisierter öffentlicher Turing-Test, um zu erkennen, ob Computer oder Mensch (en: completely automated public Turing test to tell computers and humans apart)
CPU	Prozessor (en: central processing unit)
DAC	Benutzerbestimmbare Zugriffskontrolle (en: discretionary access control)
DNS	Domain Name System
GPS	Globales Positionsbestimmungssystem
IAM	Identitäts- und Zugangsverwaltung (en: identity and access management)
IKT	Informations- und Kommunikationstechnik
ID	Zuordnungsmerkmal (en: identifier)
IDE	Integrierte Entwicklungsumgebung (en: integrated development environment)
IDS	Angriffserkennungssystem (en: intrusion detection system)
IoT	Internet der Dinge (en: Internet of Things)
IP	Internet-Protokoll (en: Internet Protocol)
IPS	Angriffsabwehrsystem (en: intrusion prevention system)
IT	Informationstechnologie
ISMS	Informationssicherheitsmanagementsystem
MAC	Systembestimmte Zugriffskontrolle (en: mandatory access control)
NTP	Netzwerkzeit-Protokoll (en: network time protocol)
DSFA	Datenschutz-Folgenabschätzung
pbD	personenbezogene Daten
PIN	Persönliche Identifikationsnummer
PKI	Public-Key-Infrastruktur
PTP	Precision Time Protocol

RBAC	rollenbasierte Zugriffskontrolle (en: role-based access control)
RPO	Wiederherstellungspunkt (en: recovery point objective)
RTO	Wiederherstellungsdauer (en: recovery time objective)
SAST	Statische Anwendungssicherheitstests
SD	Speichermedium (en: secure digital)
SDN	Software-defined Networking
SD-WAN	automatisiertes, programmierbares Weitverkehrsnetz (en: software-defined wide area networking)
SIEM	Sicherheitsinformations- und Ereignismanagement (en: security information and event management)
SMS	Kurznachrichtendienst (en: short message service)
SQL	Strukturierte Abfragesprache (en: structured query language)
SSO	einmalige Anmeldung (en: single sign on)
SWID	Softwareidentifikation
UEBA	User and Entity Behavior Analytics
USV	Unterbrechungsfreie Stromversorgung
URL	Uniform Resource Locator
USB	Universal Serial Bus
VM	Virtuelle Maschine
VPN	Virtuelles privates Netzwerk
WiFi	Zertifizierung durch Wi-Fi-Allianz (en: wireless fidelity)

4 Aufbau dieses Dokuments

4.1 Abschnitte

Dieses Dokument ist wie folgt strukturiert:

- Organisatorische Maßnahmen (Abschnitt 5);
- Personenbezogene Maßnahmen (Abschnitt 6);
- Physische Maßnahmen (Abschnitt 7);
- Technologische Maßnahmen (Abschnitt 8).

Es gibt 2 informative Anhänge:

- Anhang A — Verwendung von Attributen
- Anhang B — Übereinstimmung mit ISO/IEC 27002:2013

In Anhang A wird erläutert, wie eine Organisation Attribute (siehe 4.2) verwenden kann, um ihre eigenen Sichten auf der Grundlage der in diesem Dokument definierten oder von ihr selbst erstellten Kontrollattribute zu erstellen.

Anhang B zeigt die Übereinstimmung zwischen den Maßnahmen in dieser Ausgabe von ISO/IEC 27002 und der vorherigen Ausgabe 2013.

4.2 Themen und Attribute

Die in Abschnitt 5 bis Abschnitt 8 vorgenommene Kategorisierung der Maßnahmen wird als Themen bezeichnet.

Die Maßnahmen werden in folgende Kategorien eingeteilt:

- a) Menschen, wenn sie einzelne Menschen betreffen;
- b) physisch, wenn sie physische Objekte betreffen;
- c) technologisch, wenn sie die Technik betreffen;
- d) ansonsten werden sie als organisatorisch eingestuft.

Die Organisation kann Attribute verwenden, um verschiedene Sichten zu erstellen, bei denen es sich um verschiedene Kategorisierungen von Maßnahmen aus einer anderen Perspektive als der der Themen handelt. Attribute können zum Filtern, Sortieren oder zur Darstellung von Maßnahmen in verschiedenen Sichten für unterschiedliche Zielgruppen verwendet werden. Anhang A erläutert, wie dies erreicht werden kann, und enthält ein Beispiel für eine Sicht.

Als Beispiel wurde jede Maßnahme in diesem Dokument mit fünf Attributen mit entsprechenden Attributwerten (mit vorangestellter „#“, um sie durchsuchbar zu machen) verbunden, und zwar wie folgt:

a) Maßnahmenart

Die Maßnahmenart ist ein Attribut für die Sicht der Maßnahmen unter dem Gesichtspunkt, wann und wie die Maßnahme das Risiko in Bezug auf das Auftreten eines Informationssicherheitsvorfalls verändert. Attributwerte bestehen aus Präventiv (die Maßnahme, die das Auftreten eines Informationssicherheitsvorfalls verhindern soll), Detektiv (die Maßnahme wirkt, wenn ein Informationssicherheitsvorfall auftritt) und Korrektiv (die Maßnahme wirkt, nachdem ein Informationssicherheitsvorfall auftritt).

b) Informationssicherheitseigenschaften

Die Informationssicherheitseigenschaften sind ein Attribut, mit dem Maßnahmen unter dem Gesichtspunkt betrachtet werden können, welches Merkmal der Informationen durch die Maßnahme geschützt werden soll. Die Attributwerte bestehen aus Vertraulichkeit, Integrität und Verfügbarkeit.

c) Konzepte zur Cybersicherheit

Das Attribut „Cybersicherheitskonzepte“ dient dazu, Maßnahmen aus der Perspektive der Zuordnung von Maßnahmen zu Cybersicherheitskonzepten zu betrachten, die in dem in ISO/IEC TS 27110 beschriebenen Cybersicherheitsrahmenwerk definiert sind. Die Attributwerte bestehen aus Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

d) Betriebsfähigkeit

Das Attribut „Betriebsfähigkeit“ dient dazu, die Maßnahmen aus der Perspektive der Informationssicherheitsfähigkeiten zu betrachten. Die Attributwerte umfassen Governance, Asset_Management, Informationsschutz, Sicherheit der Humanressourcen, physische Sicherheit, System- und Netzwerksicherheit, Anwendungssicherheit, sichere Konfiguration, Identitäts- und Zugangsverwaltung, Bedrohungs- und Schwachstellenmanagement, Kontinuität, Sicherheit der Lieferantenbeziehungen, Recht und Compliance, Informationssicherheits-Ereignis-Management und Vertrauenswürdigkeit in Bezug auf die Informationssicherheit.

e) Sicherheitsdomänen

Sicherheitsdomänen ist ein Attribut, mit dem Maßnahmen aus der Perspektive von vier Informationssicherheitsdomänen betrachtet werden können: „Governance und Ökosystem“ umfasst „Governance und Risikomanagement für die Sicherheit von Informationssystemen“ und „Cybersicherheitsmanagement im Ökosystem“ (einschließlich interner und externer interessierter Parteien); „Schutz“ umfasst „IT-Sicherheitsarchitektur“, „IT-Sicherheitsverwaltung“, „Identitäts- und Zugangssverwaltung“, „IT-Sicherheitswartung“ und „physische und umgebungsbezogene Sicherheit“; „Verteidigung“ umfasst „Erkennung“ und „Management von Computersicherheitsvorfällen“; „Resilienz“ umfasst „Betriebskontinuität“ und „Krisenmanagement“. Die Attributwerte bestehen aus Governance_und_Ökosystem, Schutz, Verteidigung und Resilienz.

Die in diesem Dokument aufgeführten Attribute wurden ausgewählt, weil sie als allgemein genug angesehen werden, um von verschiedenen Arten von Organisationen verwendet werden zu können. Organisationen können sich dafür entscheiden, eines oder mehrere der in diesem Dokument aufgeführten Attribute zu ignorieren. Sie können auch eigene Attribute (mit den entsprechenden Attributwerten) anlegen, um ihre eigenen Organisationssichten zu erstellen. Abschnitt A.2 enthält Beispiele für solche Attribute.

4.3 Maßnahmengestaltung

Die Gestaltung für jede Maßnahme enthält Folgendes:

- **Maßnahmenüberschrift:** Kurzbezeichnung der Maßnahme;
- **Attributtabelle:** Eine Tabelle zeigt die Werte der einzelnen Attribute für die jeweilige Maßnahme;
- **Maßnahme:** Wie die Maßnahme aussieht;
- **Zweck:** Warum die Maßnahme umgesetzt werden sollte;
- **Leitfaden:** Wie die Maßnahme umgesetzt werden sollte;
- **Weitere Informationen:** Erläuternder Text oder Verweisungen auf andere einschlägige Dokumente.

Für einige Maßnahmen werden im Text der Leitfäden Unterüberschriften verwendet, um die Lesbarkeit zu erleichtern, wenn die Leitfäden lang sind und mehrere Themen behandeln. Diese Überschriften werden nicht unbedingt in allen Leitfäden verwendet. Unterüberschriften sind unterstrichen.

5 Organisatorische Maßnahmen

5.1 Informationssicherheitsrichtlinien

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Ökosystem #Resilienz

Maßnahme

Informationssicherheitspolitik und themenspezifische Richtlinien sollten definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

Zweck

Sicherstellung der fortwährenden Eignung, Angemessenheit und Wirksamkeit der Managementanweisungen und der Unterstützung für die Informationssicherheit in Übereinstimmung mit den geschäftlichen, rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen.

Leitfaden

Die Organisation sollte auf höchster Ebene eine „Informationssicherheitspolitik“ definieren, die von der obersten Leitung genehmigt ist und einen Ansatz zur Bewältigung der Informationssicherheit festlegt.

Die Informationssicherheitspolitik sollte die Anforderungen berücksichtigen, die sich aus folgenden Punkten ergeben:

- a) Geschäftsstrategie und Anforderungen;
- b) Vorschriften, Gesetze und Verträge;
- c) die aktuellen und voraussichtlichen Informationssicherheitsrisiken und -bedrohungen.

Die Informationssicherheitspolitik sollte Aussagen enthalten über:

- a) Definition der Informationssicherheit;
- b) Informationssicherheitsziele oder den Rahmen zum Festlegen von Informationssicherheitszielen;
- c) Grundsätze, um alle Aktivitäten in Bezug auf Informationssicherheit lenken zu können;
- d) Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit;
- e) Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems;
- f) Zuordnung von Verantwortlichkeiten zu definierten Rollen für die Handhabung von Informationssicherheit;
- g) Verfahren für den Umgang mit Befreiungen und Ausnahmen.

Die oberste Leitung sollte alle Änderungen an der Informationssicherheitspolitik genehmigen.

Auf tieferer Ebene sollte die Informationssicherheitspolitik bei Bedarf durch themenspezifische Richtlinien unterstützt werden, die zusätzlich die Umsetzung von Maßnahmen zur Informationssicherheit anordnen. Themenspezifische Richtlinien sind in der Regel so aufgebaut, dass die Bedürfnisse gewisser Zielgruppen einer Organisation angesprochen oder bestimmte Sicherheitsbereiche abgedeckt werden. Themenspezifische Richtlinien sollten auf die Informationssicherheitspolitik der Organisation abgestimmt sein und diese ergänzen.

Beispiele für solche Themen sind unter anderen:

- a) Zugangssteuerung;
- b) physische und umgebungsbezogene Sicherheit;
- c) Verwaltung der Werte;
- d) Informationsübertragung;
- e) sichere Konfiguration und Handhabung von Benutzerendgeräten;
- f) Netzwerksicherheit;
- g) Handhabung von Informationssicherheitsvorfällen;
- h) Datensicherung;
- i) Kryptographie und Schlüsselverwaltung;
- j) Informationsklassifizierung und deren Handhabung;
- k) Handhabung von technischen Schwachstellen;
- l) sichere Entwicklung.

Die Verantwortung für die Entwicklung, Überprüfung und Genehmigung der themenspezifischen Richtlinien sollte dem zuständigen Personal auf der Grundlage seiner entsprechenden Befugnisse und fachlichen Kompetenz übertragen werden. Die Überprüfung sollte eine Bewertung von Möglichkeiten zur Verbesserung der Informationssicherheitspolitik der Organisation und themenspezifischer Richtlinien sowie die Verwaltung der Informationssicherheit als Reaktion auf Änderungen umfassen:

- a) die Geschäftsstrategie des Unternehmens;
- b) das technische Umfeld der Organisation;
- c) Vorschriften, Satzungen, Gesetze und Verträge;
- d) Informationssicherheitsrisiken;
- e) das aktuelle und voraussichtliche Bedrohungsumfeld der Informationssicherheit;
- f) Lehren aus Ereignissen und Vorfällen im Bereich der Informationssicherheit.

Bei der Überprüfung der Informationssicherheitspolitik und der themenspezifischen Richtlinien sollten die Ergebnisse von Managementprüfungen und Audits berücksichtigt werden. Die Überprüfung und Aktualisierung anderer damit zusammenhängender Richtlinien sollte in Betracht gezogen werden, wenn eine Richtlinie geändert wird, um die Konsistenz zu wahren.

Die Informationssicherheitspolitik und die themenspezifischen Richtlinien sollten dem zuständigen Personal und den interessierten Kreisen in einer Form mitgeteilt werden, die relevant, zugänglich und für den vorgesehenen Leser verständlich ist. Von den Empfängern der Richtlinien sollte verlangt werden, dass sie bestätigen, die Richtlinien verstanden zu haben und sie gegebenenfalls einzuhalten. Die Organisation kann die Formate und Bezeichnungen dieser Richtlinien dokumente festlegen, die ihren Bedürfnissen entsprechen. In einigen Organisationen können die Informationssicherheitspolitik und die themenspezifischen Richtlinien in einem einzigen Dokument zusammengefasst werden. Die Organisation kann diese themenspezifischen Richtlinien als Normen, Direktiven, Richtlinien oder andere bezeichnen.

Wird die Informationssicherheitspolitik oder eine themenspezifische Richtlinie außerhalb der Organisation verbreitet, sollte darauf geachtet werden, dass vertrauliche Informationen nicht missbräuchlich weitergegeben werden.

Tabelle 1 veranschaulicht die Unterschiede zwischen der Informationssicherheitspolitik und der themenspezifischen Richtlinie.

Tabelle 1 — Unterschiede zwischen Informationssicherheitspolitik und themenspezifischer Richtlinie

	Informationssicherheitspolitik	Themenspezifische Richtlinie
Detailgenauigkeit	allgemein oder hochrangig	spezifisch und ausführlich
Dokumentiert und formell genehmigt durch	oberste Leitung	angemessene Managementebene

Weitere Informationen

Themenspezifische Richtlinien können von Organisation zu Organisation unterschiedlich sein.

5.2 Informationssicherheitsrollen und -verantwortlichkeiten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Ökosystem #Schutz #Resilienz

Maßnahme

Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit sollten entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.

Zweck

Schaffung einer definierten, genehmigten und verstandenen Struktur für die Implementierung, den Betrieb und die Verwaltung der Informationssicherheit innerhalb der Organisation.

Leitfaden

Die Zuweisung von Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit sollte in Übereinstimmung mit der Informationssicherheitspolitik und den themenspezifischen Richtlinien erfolgen (siehe 5.1). Die Organisation sollte Zuständigkeiten für folgende Bereiche festlegen und verwalten:

- a) Schutz von Informationen und anderen damit verbundenen Werten;
- b) Durchführung spezifischer Verfahren der Informationssicherheit;
- c) Risikomanagementaktivitäten im Bereich der Informationssicherheit und insbesondere die Übernahme von Restrisiken (z. B. gegenüber den Risikoverantwortlichen);
- d) das gesamte Personal nutzt die Informationen einer Organisation und andere damit verbundene Werte.

Diese Verantwortlichkeiten sollten soweit erforderlich um detaillierte Anleitungen für bestimmte Standorte und Einrichtungen der Informationsverarbeitung erweitert werden. Personen mit zugeordneten Verantwortlichkeiten für Informationssicherheit können anderen Sicherheitsaufgaben zuweisen. Jedoch bleiben sie verantwortlich und sollten feststellen, ob alle übertragenen Aufgaben ordnungsgemäß durchgeführt wurden.

Jeder Sicherheitsbereich, für den einzelne Personen verantwortlich sind, sollte definiert, dokumentiert und kommuniziert werden. Berechtigungsebenen sollten definiert und dokumentiert werden. Personen, die eine bestimmte Aufgabe im Bereich der Informationssicherheit übernehmen, sollten über die für diese Aufgabe erforderlichen Kenntnisse und Fähigkeiten verfügen und dabei unterstützt werden, sich über die Entwicklungen auf dem Laufenden zu halten, die mit dieser Aufgabe zusammenhängen und für die Erfüllung der mit dieser Aufgabe verbundenen Pflichten erforderlich sind.

Weitere Informationen

Viele Organisationen ernennen einen Manager für Informationssicherheit, der die Gesamtverantwortung für Entwicklung und Umsetzung der Informationssicherheit übernimmt und die Identifizierung von Risiken und Kontrollmechanismen zur Risikominderung unterstützt.

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

Je nach Größe und Ressourcenausstattung einer Organisation kann die Informationssicherheit durch spezielle Funktionen oder durch Aufgaben abgedeckt werden, die zusätzlich zu den bestehenden Funktionen ausgeführt werden.

5.3 Aufgabendrennung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Governance #Identitäts- und Zugangsverwaltung	#Governance_und_Ökosystem

Maßnahme

Sich widersprechende Aufgaben und Verantwortungsbereiche sollten voneinander getrennt werden.

Zweck

Verringerung des Risikos von Betrug, Fehlern und Umgehung von Informationssicherheitsmaßnahmen.

Leitfaden

Die Trennung von Aufgaben und Verantwortungsbereichen zielt darauf ab, widersprüchliche Aufgaben zwischen verschiedenen Personen zu trennen, um zu verhindern, dass eine Person potentiell widersprüchliche Aufgaben im Alleingang ausführt.

Die Organisation sollte festlegen, welche Aufgaben und Verantwortungsbereiche getrennt werden müssen. Im Folgenden werden Beispiele für Tätigkeiten genannt, die eine Trennung erfordern können:

- a) Initiierung, Genehmigung und Durchführung einer Änderung;
- b) Beantragung, Genehmigung und Umsetzung von Zugangsrechten;
- c) Gestaltung, Implementierung und Überprüfung eines Codes;
- d) Entwicklung von Software und Verwaltung von Produktionssystemen;
- e) Nutzung und Verwaltung von Anwendungen;
- f) Nutzung von Anwendungen und Verwaltung von Datenbanken;
- g) Gestaltung, Auditierung und Sicherstellung von Informationssicherheitsmaßnahmen.

Die Möglichkeit von Absprachen sollte bei der Gestaltung der Trennungsmaßnahmen berücksichtigt werden. Für kleine Organisationen kann Aufgabentrennung nur mit Schwierigkeiten zu erreichen sein, das Prinzip sollte aber so weit wie möglich und praktikabel angewandt werden. Falls Aufgabentrennung nur schwer durchführbar ist, sollten andere Maßnahmen wie Überwachung von Tätigkeiten, Prüfpfade und Leitungsaufsicht in Betracht gezogen werden.

Bei der Verwendung von rollenbasierten Zugangssteuerungssystemen sollte darauf geachtet werden, dass Personen keine widersprüchlichen Rollen zugewiesen werden. Bei einer großen Anzahl von Rollen sollte das Unternehmen den Einsatz automatisierter Tools in Betracht ziehen, um Konflikte zu erkennen und deren Beseitigung zu erleichtern. Rollen sollten sorgfältig definiert und bereitgestellt werden, um Zugriffsprobleme zu minimieren, wenn eine Rolle entfernt oder neu zugewiesen wird.

Weitere Informationen

Keine weiteren Informationen.

5.4 Verantwortlichkeiten der Leitung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Ökosystem

Maßnahme

Die Leitung sollte von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.

Zweck

Es soll sichergestellt werden, dass das Management seine Rolle im Bereich der Informationssicherheit versteht und Maßnahmen ergreift, die sicherstellen, dass das gesamte Personal seiner Verantwortung für die Informationssicherheit nachkommt.

Leitfaden

Die Leitung sollte nachweisen, dass die Informationssicherheitspolitik, die themenspezifischen Richtlinien, Verfahren und Informationssicherheitsmaßnahmen unterstützt werden.

Die Verantwortlichkeiten der Leitung sollten unter anderem beinhalten, dass das Personal:

- über seine Rollen und Verantwortlichkeiten in der Informationssicherheit informiert wird, bevor es Zugang zu den Informationen der Organisation und anderen damit verbundenen Werten erhält;
- Leitfäden erhält, die die Erwartungen an seine Rolle in der Informationssicherheit innerhalb der Organisation darlegt;
- den Auftrag hat, die Informationssicherheitspolitik und den themenspezifischen Richtlinien der Organisation gerecht zu werden;
- ein Informationssicherheitsbewusstsein erreicht, das seinen Rollen und Verantwortlichkeiten in der Organisation entspricht (siehe 6.3);
- Einhaltung der Beschäftigungsbedingungen, des Vertrages oder der Vereinbarung, einschließlich der Informationssicherheitspolitik der Organisation und geeigneten Arbeitsmethoden;
- auch in Zukunft angemessene Fähigkeiten und Qualifikationen im Bereich der Informationssicherheit besitzt und ständig beruflich weitergebildet wird;
- soweit praktikabel, vertraulich über Verletzungen gegen die Informationssicherheitspolitik, themenspezifische Richtlinien oder Verfahren für die Informationssicherheit Bericht erstatten kann („whistleblowing“). Hierbei kann es sich um anonyme Meldungen handeln oder um Bestimmungen, die sicherstellen, dass die Identität des Berichterstatters nur denjenigen bekannt ist, die sich mit solchen Meldungen befassen müssen;
- über angemessene Ressourcen und Projektplanungszeit für die Implementierung der sicherheitsrelevanten Prozesse und Maßnahmen in der Organisation verfügt.

Weitere Informationen

Keine weiteren Informationen.

5.5 Kontakt mit Behörden

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung #Resilienz

Maßnahme

Die Organisation sollte mit den zuständigen Behörden Kontakt aufnehmen und halten.

Zweck

Sicherstellung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit zwischen der Organisation und den zuständigen Rechts-, Regulierungs- und Aufsichtsbehörden.

Leitfaden

Die Organisation sollte festlegen, wann und durch wen Behörden (z. B. Strafverfolgungs-, Regulierungs- und Aufsichtsbehörden) benachrichtigt werden und wie erkannte Informationssicherheitsvorfälle rechtzeitig gemeldet werden.

Kontakte mit Behörden sollten auch dazu genutzt werden, das Verständnis für die aktuellen und zukünftigen Erwartungen dieser Behörden (z. B. geltende Informationssicherheitsvorschriften) zu erleichtern.

Weitere Informationen

Organisationen, die angegriffen werden, können die Behörden auffordern, Schritte gegen die Angriffsquelle zu ergreifen.

Die Pflege solcher Kontakte kann eine Anforderung für die Unterstützung bei Informationssicherheitsvorfällen (siehe 5.24 bis 5.28) oder für den Notfallplanungsprozess und den Prozess zur Aufrechterhaltung der Betriebsfähigkeit (siehe 5.29 und 5.30) sein. Kontakte mit Aufsichtsbehörden helfen auch bei der Vorwegnahme und Vorbereitung anstehender Änderungen von geltenden Gesetzen oder Regulierungen, die die Organisation beeinflussen. Kontakte mit anderen Behörden umfassen auch Versorgungseinrichtungen, wie Notdienste, Stromversorgungsunternehmen, Hilfs- und Rettungsdienste [z. B. Feuerwehr (in Verbindung mit Business Continuity), Telekommunikationsanbieter (in Verbindung mit Leitungsverlegung und Verfügbarkeit) und Wasserversorger (in Verbindung mit Kühleinrichtungen für Geräte)].

5.6 Kontakt mit speziellen Interessensgruppen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung

Maßnahme

Die Organisation sollte Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden herstellen und pflegen.

Zweck

Sicherstellung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit.

Leitfaden

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

- die Kenntnis über beste Praktiken zu verbessern und über relevante Sicherheitsinformationen auf dem Laufenden zu bleiben;
- sicherzustellen, dass das Verständnis im Umfeld der Informationssicherheit aktuell ist;
- um rechtzeitig Warnungen, Hinweise und Patches zum Schutz vor Angriffen und Schwachstellen zu erhalten;
- um Zugang zu Fachberatung über Informationssicherheit zu erhalten;
- um Information über neue Technologien, Produkte, Dienste, Bedrohungen oder Schwachstellen auszutauschen;
- um geeignete Verbindungsstellen beim Umgang mit Informationssicherheitsvorfällen zu bieten (siehe 5.24 bis 5.28).

Weitere Informationen

Keine weiteren Informationen.

5.7 Bedrohungsintelligenz

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Erkennen #Reagieren	#Bedrohungs_und_Schwachstellenmanagement	#Verteidigung #Resilienz

Maßnahme

Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.

Zweck

Sensibilisierung für die Bedrohungslage des Unternehmens, damit geeignete Maßnahmen zur Risikominderung ergriffen werden können.

Leitfaden

Informationen über bestehende oder neu auftretende Bedrohungen werden erhoben und ausgewertet, um:

- a) fundierte Maßnahmen zu erleichtern, um zu verhindern, dass die Bedrohungen der Organisation Schaden zufügen;
- b) die Auswirkungen solcher Bedrohungen zu verringern.

Bedrohungsdaten lassen sich in drei Schichten unterteilen, die alle berücksichtigt werden sollten:

- a) strategische Bedrohungsanalyse: Austausch von Informationen über die sich verändernde Bedrohungslandschaft (z. B. Arten von Angreifern oder Angriffen);
- b) taktische Bedrohungsdaten: Informationen über die Methoden, Werkzeuge und Technologien der Angreifer;
- c) operative Bedrohungsdaten: Einzelheiten zu bestimmten Angriffen, einschließlich technischer Indikatoren.

Bedrohungsanalyse sollte sein:

- a) relevant (d. h. im Zusammenhang mit dem Schutz der Organisation);
- b) aufschlussreich ist (d. h. der Organisation ein genaues und detailliertes Verständnis der Bedrohungslandschaft vermittelt);
- c) kontextbezogen, um ein Situationsbewusstsein zu schaffen (d. h. Hinzufügen von Kontext zu den Informationen auf der Grundlage des Zeitpunkts der Ereignisse, des Ortes, an dem sie auftreten, früherer Erfahrungen und der Häufigkeit in ähnlichen Organisationen);
- d) umsetzbar (d. h. die Organisation kann schnell und effektiv auf Informationen reagieren).

Die Bedrohungsanalyse sollte Folgendes umfassen:

- a) Festlegung von Zielen für die Erstellung von Bedrohungsdaten;
- b) Ermittlung, Sicherheitsüberprüfung und Auswahl interner und externer Informationsquellen, die erforderlich und geeignet sind, um die für die Erstellung von Bedrohungsdaten erforderlichen Informationen zu liefern;
- c) Erhebung von Informationen aus ausgewählten Quellen, die sowohl intern als auch extern sein können;
- d) Verarbeitung der erhobenen Informationen, um sie für die Analyse vorzubereiten (z. B. durch Übersetzung, Formatierung oder Bestätigung der Informationen);

- e) Analyse von Informationen, um zu verstehen, wie sie mit dem Unternehmen zusammenhängen und für dieses von Bedeutung sind;
- f) Kommunikation und Weitergabe der Informationen an die betroffenen Personen in einem verständlichen Format.

Die Informationen zu den Bedrohungen sollten analysiert und später genutzt werden:

- a) durch die Implementierung von Prozessen zur Einbeziehung von Informationen aus Bedrohungsdatenquellen in die Risikomanagementprozesse der Organisation für die Informationssicherheit;
- b) als zusätzlicher Beitrag zu technischen Präventiv- und Detektivmaßnahmen wie Firewalls, Einbruchmeldeanlagen oder Anti-Schadsoftware-Lösungen;
- c) als Input für die Prozesse und Techniken der Informationssicherheitsprüfung.

Die Organisation sollte Bedrohungsdaten mit anderen Organisationen auf gegenseitiger Basis austauschen, um die Bedrohungsdaten insgesamt zu verbessern.

Weitere Informationen

Organisationen können Bedrohungsdaten nutzen, um Bedrohungen zu verhindern, zu erkennen oder darauf zu reagieren. Organisationen können Bedrohungsdaten selbst erstellen, erhalten und nutzen aber in der Regel Bedrohungsdaten aus anderen Quellen.

Bedrohungsdaten werden häufig von unabhängigen Anbietern oder Beratern, Regierungsbehörden oder kooperativen Bedrohungsdatengruppen bereitgestellt.

Die Wirksamkeit von Maßnahmen wie 5.25, 8.7, 8.16 oder 8.23 hängt von der Qualität der verfügbaren Bedrohungsdaten ab.

5.8 Informationssicherheit im Projektmanagement

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Governance	#Governance_und_Ökosystem #Schutz

Maßnahme

Die Informationssicherheit sollte in das Projektmanagement integriert werden.

Zweck

Sicherstellung, dass Informationssicherheitsrisiken im Zusammenhang mit Projekten und Leistungen im Projektmanagement während des gesamten Projektlebenszyklus wirksam behandelt werden.

Leitfaden

Die Informationssicherheit sollte in das Projektmanagement integriert werden, um sicherzustellen, dass die Risiken der Informationssicherheit im Rahmen des Projektmanagements behandelt werden. Dies kann auf jede Art von Projekt angewandt werden, unabhängig von dessen Komplexität, Größe, Dauer, Disziplin oder Anwendungsbereich (z. B. ein Projekt für einen Kerngeschäftsprozess, IKT, Gebäudemanagement oder andere unterstützende Prozesse).

Das verwendete Projektmanagement sollte verlangen, dass:

- a) die Risiken für die Informationssicherheit in einem frühen Stadium und regelmäßig als Teil der Projektrisiken während des gesamten Projektlebenszyklus bewertet und behandelt werden;
- b) Anforderungen an die Informationssicherheit [z. B. Anforderungen an die Anwendungssicherheit (8.26), Anforderungen an die Einhaltung von Rechten an geistigem Eigentum (5.32) usw.] in den frühen Phasen der Projekte behandelt werden;
- c) die Risiken für die Informationssicherheit in einem frühen Stadium und regelmäßig als Teil der Projektrisiken während des gesamten Projektlebenszyklus bewertet und behandelt werden;
- d) die Fortschritte bei der Behandlung von Informationssicherheitsrisiken überprüft werden und die Wirksamkeit der Behandlung bewertet und getestet wird.

Die Angemessenheit der Überlegungen und Aktivitäten zur Informationssicherheit sollte in festgelegten Phasen von geeigneten Personen oder Leitungsgremien, wie dem Projektleitungsausschuss, überprüft werden.

Die Zuständigkeiten und Befugnisse für die Informationssicherheit, die für das Projekt relevant sind, sollten definiert und bestimmten Rollen zugewiesen werden.

Die Anforderungen an die Informationssicherheit für die im Rahmen des Projekts zu liefernden Produkte oder Dienstleistungen sollten mit Hilfe verschiedener Verfahren ermittelt werden, einschließlich der Ableitung von Konformitätsanforderungen aus der Informationssicherheitspolitik, themenspezifischen Richtlinien und Vorschriften. Weitere Anforderungen an die Informationssicherheit lassen sich aus Aktivitäten wie der Modellierung von Bedrohungen, der Überprüfung von Vorfällen, der Verwendung von Schwellenwerten für Schwachstellen oder der Notfallplanung ableiten, wodurch sichergestellt wird, dass die Architektur und die Gestaltung von Informationssystemen gegen bekannte Bedrohungen auf der Grundlage des betrieblichen Umfelds geschützt sind.

Die Anforderungen an die Informationssicherheit sollten für alle Arten von Projekten festgelegt werden, nicht nur für IKT-Entwicklungsprojekte. Bei der Festlegung dieser Anforderungen sollten auch die folgenden Punkte berücksichtigt werden:

- a) um welche Informationen es sich handelt (Informationsbestimmung), welche Informationssicherheitsanforderungen damit verbunden sind (Klassifizierung; siehe 5.12) und welche potentiellen negativen geschäftlichen Auswirkungen sich aus einer fehlenden angemessenen Sicherheit ergeben können;
- b) den erforderlichen Schutzbedarf von Informationen und anderen damit verbundenen Werten, insbesondere in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit;
- c) das erforderliche Vertrauensniveau oder die erforderliche Vertrauenswürdigkeitsstufe in Bezug auf die von den Entitäten angegebene Identität zur Ableitung der Anforderungen hinsichtlich der Authentifizierung;

- d) Zugangserteilungs- und -berechtigungsprozesse für Kunden und andere potentielle geschäftliche Benutzer sowie für privilegierte oder technische Benutzer wie relevante Projektmitglieder, potentielles Betriebspersonal oder externe Lieferanten;
- e) die Informierung von Benutzern über ihre Pflichten und Verantwortlichkeiten;
- f) die aus den Geschäftsabläufen abgeleiteten Anforderungen wie die Protokollierung und Überwachung von Transaktionen sowie Anforderungen bezüglich der Nichtabstreitbarkeit;
- g) die Anforderungen, die durch andere Informationssicherheitsmaßnahmen gegeben sind (z.B. Schnittstellen zu Protokollierungs- und Überwachungssystemen oder Systemen zur Erkennung von Datenverlusten);
- h) die Einhaltung der rechtlichen, gesetzlichen, behördlichen und vertraglichen Rahmenbedingungen, in denen die Organisation tätig ist;
- i) Vertrauensniveau oder Vertrauenswürdigkeitsstufe, das/die erforderlich ist, damit Dritte die Informationssicherheitspolitik der Organisation und die themenspezifischen Richtlinien einhalten, einschließlich der einschlägigen Sicherheitsabschnitte in allen Vereinbarungen oder Verträgen.

Weitere Informationen

Der Projektentwicklungsansatz, wie z. B. der Wasserfall-Lebenszyklus oder der agile Lebenszyklus, sollte die Informationssicherheit in einer strukturierten Weise unterstützen, die je nach Art des Projekts an den bewerteten Schweregrad der Informationssicherheitsrisiken angepasst werden kann. Eine frühzeitige Berücksichtigung der Anforderungen an die Informationssicherheit für das Produkt oder die Dienstleistung (z. B. in der Planungs- und Gestaltungsphase) kann zu effektiveren und kosteneffizienteren Lösungen für Qualität und Informationssicherheit führen. ISO 21500 und ISO 21502 bieten eine Anleitung zu Konzepten und Prozessen des Projektmanagements, die für die Durchführung von Projekten wichtig sind.

ISO/IEC 27005 enthält Richtlinien zur Anwendung von Risikomanagement-Prozessen für die Ermittlung von Sicherheitsmaßnahmen zur Einhaltung der Informationssicherheitsanforderungen.

5.9 Inventar der Informationen und anderen damit verbundenen Werten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Asset_Management	#Governance_und_Ökosystem #Schutz

Maßnahme

Ein Inventar der Informationen und anderen damit verbundenen Werten, einschließlich der Eigentümer, sollte erstellt und gepflegt werden.

Zweck

Identifizierung der Informationen und anderer zugehöriger Werte der Organisation, um deren Informationssicherheit zu wahren und entsprechende Eigentumsrechte zuzuweisen.

Leitfaden

Inventar

Die Organisation sollte ihre Informationen und andere zugehörige Werte identifizieren und deren Bedeutung in Bezug auf die Informationssicherheit bestimmen. Die Dokumentation sollte in eigenen oder ggf. bestehenden Inventaren aufbewahrt werden.

Das Inventar der Informationen und anderer zugehöriger Werte sollte genau, aktuell und konsistent sowie mit anderen Inventaren abgestimmt sein. Zu den Optionen zur Sicherstellung der Genauigkeit eines Inventars von Informationen und anderen zugehörigen Werten gehören:

- a) Durchführung regelmäßiger Überprüfungen der identifizierten Informationen und anderer zugehöriger Vermögenswerte anhand des Inventars der Vermögenswerte;
- b) automatische Erzwingung einer Inventaraktualisierung bei der Installation, Änderung oder Entfernung eines Wertes.

Der Ort, an dem sich ein Wert befindet, sollte gegebenenfalls in das Inventar aufgenommen werden.

Das Inventar muss nicht eine einzige Liste von Informationen und anderen zugehörigen Werten sein. In Anbetracht der Tatsache, dass das Inventar von den relevanten Funktionen gepflegt werden sollte, kann es als eine Reihe dynamischer Inventare angesehen werden, wie z. B. Inventare für Informationswerte, Hardware, Software, virtuelle Maschinen (VMs), Einrichtungen, Personal, Kompetenzen, Fähigkeiten und Aufzeichnungen.

Jeder Wert sollte in Übereinstimmung mit der Klassifizierung der zu diesem Wert gehörenden Informationen (siehe 5.12) klassifiziert werden.

Die Granularität des Inventars von Informationen und anderen zugehörigen Werten sollte den Bedürfnissen der Organisation angemessen sein. Manchmal ist es aufgrund der Beschaffenheit von Werten im Lebenszyklus von Informationen nicht möglich, bestimmte Instanzen von Werten zu dokumentieren. Ein Beispiel für einen kurzlebigen Wert ist eine VM-Instanz, deren Lebenszyklus von kurzer Dauer sein kann.

Zuständigkeit

Für die identifizierten Informationen und andere zugehörige Werte sollte die Zuständigkeit für den Wert einer Person oder einer Gruppe zugewiesen und die Klassifizierung festgelegt werden (siehe 5.12, 5.13). Ein Prozess zur Sicherstellung einer zeitnahen Bestimmung der Zuständigkeit für Werte sollte umgesetzt werden. Die Zuständigkeit sollte zugewiesen werden, wenn Werte geschaffen oder auf die Organisation übertragen werden. Die Zuständigkeit für Werte sollte bei Bedarf neu zugewiesen werden, wenn die derzeitigen Eigentümer ausscheiden oder ihre Funktion wechseln.

Pflichten des Eigentümers

Der Eigentümer eines Werts sollte für die ordnungsgemäße Verwaltung eines Werts über den gesamten Lebenszyklus des Werts verantwortlich sein und sicherstellen, dass:

- a) Informationen und andere damit verbundene Werte inventarisiert werden;
- b) Informationen und andere damit verbundene Werte angemessen klassifiziert und geschützt werden;
- c) die Klassifizierung periodisch überprüft wird;
- d) Komponenten zur Unterstützung von Technologiewerten aufgelistet und miteinander verknüpft werden, z. B. Datenbank, Speicher, Softwarekomponenten und Unterkomponenten;

- e) Anforderungen für den zulässigen Gebrauch von Informationen und anderen zugehörigen Werten (siehe 5.10) festgelegt werden;
- f) die Zugangsbeschränkungen der Klassifizierung entsprechen, dass sie wirksam sind und regelmäßig überprüft werden;
- g) Informationen und andere zugehörige Werte, wenn sie gelöscht oder entsorgt werden, auf sichere Weise gehandhabt und aus dem Inventar entfernt werden;
- h) sie an der Identifizierung und dem Management der mit ihren Werten verbundenen Risiken beteiligt sind;
- i) sie das Personal unterstützen, das die Aufgabe und die Verantwortung hat, ihre Informationen zu verwalten.

Weitere Informationen

Die Inventarverzeichnisse von Informationen und anderen zugehörigen Werten sind oft notwendig, um den wirksamen Schutz von Informationen sicherzustellen, und können auch aus anderen Gründen erforderlich sein, z. B. aus Gründen der Gesundheit und Sicherheit, der Versicherung oder aus finanziellen Gründen. Die Inventarverzeichnisse von Informationen und anderen zugehörigen Werten unterstützen auch das Risikomanagement, Auditaktivitäten, das Schwachstellenmanagement, die Reaktion auf Vorfälle und die Wiederherstellungsplanung.

Aufgaben und Verantwortlichkeiten können delegiert werden (z. B. an einen Verwalter, der täglich die Werte beaufsichtigt), aber die Person oder Gruppe, die sie delegiert hat, bleibt rechenschaftspflichtig.

Es kann sinnvoll sein, Gruppen von Informationen und anderen zugehörigen Werten zu benennen, die gemeinsam einen bestimmten Dienst erbringen. In diesem Fall ist der Zuständige dieses Dienstes oder dieser Dienstleistung für deren Erbringung verantwortlich, einschließlich des Einsatzes der Werte.

Siehe ISO/IEC 19770-1 für zusätzliche Informationen zum Management von IT-Werten. Siehe ISO 55001 für zusätzliche Informationen zum Asset Management.

5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Governance_und_Ökosystem #Schutz

Maßnahme

Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten sollten aufgestellt, dokumentiert und angewendet werden.

Zweck

Sicherstellung eines angemessenen Schutzes, einer angemessenen Nutzung und eines angemessenen Umgangs mit Informationen und anderen damit verbundenen Werten.

Leitfaden

Personal und sonstige Benutzer, die zu externen Parteien gehören, die Informationen und andere zugehörige Werte der Organisation nutzen oder Zugang zu ihnen haben, sollten auf die Informationssicherheitsanforderungen zum Schutz und zur Handhabung der Informationen und anderer zugehöriger Werte der Organisation hingewiesen werden. Sie sollten für ihre eigene Nutzung informationsverarbeitender Einrichtungen verantwortlich sein.

Die Organisation sollte eine themenspezifische Politik für die zulässige Nutzung von Informationen und anderen zugehörigen Vermögenswerten aufstellen und sie an alle Personen weitergeben, die Informationen und andere zugehörige Vermögenswerte nutzen oder bearbeiten. Die themenspezifische Richtlinie über den zulässigen Gebrauch sollte klare Anweisungen darüber geben, wie Einzelpersonen Informationen und andere zugehörige Werte nutzen sollen. Die themenspezifische Richtlinie sollte darlegen:

- a) erwartete und unzulässige Verhaltensweisen von Personen aus der Sicht der Informationssicherheit;
- b) zulässiger und verbotener Gebrauch von Informationen und anderen damit verbundenen Werten;
- c) Überwachungsaktivitäten, die von der Organisation durchgeführt werden.

Verfahren für den zulässigen Gebrauch sollten für den gesamten Lebenszyklus von Informationen in Übereinstimmung mit ihrer Klassifizierung (siehe 5.12) und den ermittelten Risiken erstellt werden. Die folgenden Punkte sollten dabei berücksichtigt werden:

- a) Zugriffsbeschränkungen zur Unterstützung der Schutzanforderungen für jede Klassifizierungsstufe;
- b) Pflege eines Verzeichnisses der befugten Benutzer von Informationen und anderen damit verbundenen Werten;
- c) Schutz temporärer oder dauerhafter Kopien von Informationen in einer Weise, die dem Schutz der Originalinformationen entspricht;
- d) Speicherung der mit den Informationen verbundenen Werte in Übereinstimmung mit den Herstellerspezifikationen (siehe 7.8);
- e) deutliche Kennzeichnung sämtlicher Speichermedien (elektronisch oder physikalisch) als Hinweis für den berechtigten Empfänger (siehe 7.10);
- f) Genehmigung der Veräußerung von Informationen und anderen zugehörigen Werten und unterstützte Löschverfahren (siehe 8.10).

Weitere Informationen

Es kann vorkommen, dass die betreffenden Werte nicht direkt der Organisation gehören, wie z. B. bei öffentlichen Cloud-Diensten. Die Nutzung derartiger Werte Dritter und aller mit diesen externen Werten verbundenen Werte der Organisation (z. B. Informationen, Software) sollte gegebenenfalls ermittelt und kontrolliert werden, beispielsweise durch Vereinbarungen mit Cloud-Service-Anbietern. Vorsicht sollte man auch walten lassen, wenn eine kollaborative Arbeitsumgebung genutzt wird.

5.11 Rückgabe von Werten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management	#Schutz

Maßnahme

Das Personal und gegebenenfalls andere interessierte Parteien sollten alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.

Zweck

Der Schutz der Werte der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung, eines Vertrags oder einer Vereinbarung.

Leitfaden

Der Beendigungs- oder Änderungsprozess 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 das Personal und andere interessierte Parteien, die Betriebsmittel der Organisation erwerben oder ihre eigene Ausrüstung benutzen, sollten Verfahren eingehalten werden, durch die sichergestellt ist, dass alle relevanten Informationen zurückverfolgt und an die Organisation übermittelt sowie sicher von den Betriebsmitteln gelöscht werden (siehe 7.14).

In Fällen, in denen Mitarbeiter und andere interessierte Parteien über Kenntnisse verfügen, die wichtig für den laufenden Betrieb sind, sollten diese Informationen dokumentiert und an die Organisation übermittelt werden.

Während der Kündigungsfrist und danach sollte die Organisation unbefugtes Kopieren relevanter Information (z. B. geistiges Eigentum) durch das gekündigte Personal verhindern.

Die Organisation sollte alle zurückzugebenden Informationen und andere damit zusammenhängende Werte klar identifizieren und dokumentieren, z. B.:

- Endpunktgeräte des Benutzers;
- tragbare Speichergeräte;
- Spezialausrüstung;
- Authentifizierungshardware (z. B. mechanische Schlüssel, physische Token und Smartcards) für Informationssysteme, Standorte und physische Archive;
- physische Kopien von Informationen.

Weitere Informationen

Es kann schwierig sein, Informationen über Werte zurückzugeben, die sich nicht im Besitz der Organisation befinden. In solchen Fällen ist es notwendig, die Verwendung von Informationen durch andere Informationssicherheitsmaßnahmen wie die Verwaltung von Zugriffsrechten (5.18) oder den Einsatz von Kryptographie (8.24) zu beschränken.

5.12 Klassifizierung von Information

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Informationsschutz	#Schutz #Verteidigung

Maßnahme

Informationen sollten entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.

Zweck

Sicherstellung der Identifizierung und des Verständnisses für den Schutzbedarf von Informationen entsprechend ihrer Bedeutung für die Organisation.

Leitfaden

Die Organisation sollte eine themenspezifische Richtlinie für die Klassifizierung von Informationen aufstellen und sie allen relevanten interessierten Parteien mitteilen.

Die Organisation sollte die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit im Klassifizierungsschema berücksichtigen.

Bei den Klassifizierungen und den damit verbundenen Sicherheitsmaßnahmen sollten die geschäftlichen Anforderungen für gemeinsame Nutzung oder für Einschränkung von Informationen, den Schutz der Integrität von Informationen und die Sicherstellung der Verfügbarkeit sowie den rechtlichen Anforderungen an die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen Rechnung tragen. Werte, bei denen es sich nicht um Information handelt, können auch unter Einhaltung der Klassifizierung der darin gespeicherten, von diesen verarbeiteten oder auf andere Weise gehandhabten oder geschützten Information klassifiziert werden.

Die Zuständigen der Informationen sollten für ihre Klassifizierung verantwortlich sein.

Das Klassifizierungsschema sollte Konventionen für die Klassifizierung und Kriterien zur Überprüfung der Klassifizierung nach einer gewissen Zeit beinhalten. Die Ergebnisse der Klassifizierung sollten bei Änderungen des Wertes, der Sensibilität und Betriebswichtigkeit der Informationen im Laufe des Lebenszyklus aktualisiert werden.

Das Schema sollte auf die themenspezifische Richtlinie zur Zugangssteuerung (siehe 5.1) abgestimmt sein und den spezifischen Geschäftsanforderungen der Organisation gerecht werden können.

Die Klassifizierung kann anhand des Ausmaßes der Auswirkungen bestimmt werden, die eine Kompromittierung der Informationen für das Unternehmen haben würde. Jeder im Schema festgelegten Stufe sollte eine Bezeichnung zugewiesen werden, die im Zusammenhang mit der Anwendung des Klassifizierungsschemas Sinn ergibt.

Das Schema sollte innerhalb der gesamten Organisation einheitlich sein und in die Verfahren aufgenommen werden, so dass jeder die Informationen und die damit verbundenen Werte auf die gleiche Weise klassifiziert. Auf diese Weise haben alle ein gemeinsames Verständnis der Schutzanforderungen und wenden einen angemessenen Schutz an.

Das innerhalb der Organisation verwendete Klassifizierungsschema kann sich von Schemata anderer Organisationen unterscheiden, 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. Daher sollten Vereinbarungen mit anderen Organisationen, die den Austausch von Informationen einschließen, Verfahren zur Feststellung der Klassifizierung der betreffenden Informationen und zur Interpretation der Klassifizierungsstufen anderer Organisationen vorsehen. Die Übereinstimmung zwischen verschiedenen Systemen kann durch die Suche nach Gleichwertigkeit in den zugehörigen Handhabungs- und Schutzverfahren festgestellt werden.

Weitere Informationen

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

Informationen können ihren sensiblen oder betriebswichtigen Charakter nach einer gewissen Zeitspanne verlieren. Wenn die Informationen beispielsweise öffentlich zugänglich gemacht wurden, gelten sie nicht mehr als vertraulich, aber ihre Integrität und Verfügbarkeit müssen weiterhin geschützt werden. 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 zu unzureichenden Maßnahmen führen, um die Informationen vor Kompromittierung zu schützen.

Als Beispiel kann ein Klassifizierungsschema zur Vertraulichkeit von Informationen auf dem folgenden, vierstufigen Modell beruhen:

- a) Offenlegung ist gefahrlos möglich;
- b) Offenlegung führt zu geringfügigem Schaden für den Ruf oder geringfügigen betrieblichen Auswirkungen;
- c) Offenlegung hat signifikante, kurzfristige Auswirkungen auf den Betriebsablauf oder Geschäftsziele;
- d) Offenlegung hat schwerwiegende Auswirkungen auf langfristige Geschäftsziele und gefährdet den Bestand der Organisation.

5.13 Kennzeichnung von Information

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Informationsschutz	#Verteidigung #Schutz

Maßnahme

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

Zweck

Erleichterung der Kommunikation bei der Klassifizierung von Informationen und Unterstützung der Automatisierung der Informationsverarbeitung und -verwaltung.

Leitfaden

Verfahren zur Kennzeichnung von Information sollten Information und andere zugehörige Werte in allen Formaten abdecken. Die Kennzeichnung sollte dem in 5.12 festgelegten Klassifizierungsschema Rechnung tragen. Die Kennzeichnungen sollten einfach zu erkennen sein. Die Verfahren sollten eine Anleitung bieten, wo und wie Kennzeichnungen anzubringen sind unter Berücksichtigung der Art und Weise, wie auf die Information zugegriffen wird bzw. der Umgang mit den Werten in Abhängigkeit vom jeweiligen Speichermedientyp erfolgt. Die Verfahren können Folgendes festlegen:

- Fälle, in denen auf eine Kennzeichnung verzichtet wird (z. B. bei nicht vertraulichen Informationen, um die Arbeitsbelastung zu verringern);
- wie Informationen zu kennzeichnen sind, die auf elektronischem oder physischem Wege oder in einem anderen Format übermittelt oder gespeichert werden;
- wie mit Fällen umzugehen ist, in denen eine Kennzeichnung nicht möglich ist (z. B. aufgrund technischer Beschränkungen).

Beispiele für Kennzeichnungsverfahren umfassen:

- physische Kennzeichnungen;
- Überschriften und Fußzeilen;
- Metadaten;
- Wasserzeichenmarkierung;
- Gummistempel.

Für digitale Informationen sollten Metadaten verwendet werden, um Informationen zu identifizieren, zu verwalten und zu kontrollieren, insbesondere im Hinblick auf die Vertraulichkeit. Metadaten sollten auch eine effiziente und korrekte Suche nach Informationen ermöglichen. Metadaten sollten es den Systemen erleichtern, zu interagieren und Entscheidungen auf der Grundlage der zugehörigen Klassifizierungskennzeichnung zu treffen.

Die Verfahren sollten beschreiben, wie Metadaten an Informationen angehängt werden, welche Kennzeichnungen verwendet werden und wie Daten im Einklang mit dem Informationsmodell und der IKT-Architektur der Organisation behandelt werden sollten.

Einschlägige zusätzliche Metadaten sollten von Systemen hinzugefügt werden, wenn sie Informationen in Abhängigkeit von ihren Informationssicherheitseigenschaften verarbeiten.

Das Personal und andere interessierte Parteien sollten auf die Kennzeichnungsverfahren aufmerksam gemacht werden. Das gesamte Personal sollte geschult werden, um sicherzustellen, dass die Informationen korrekt gekennzeichnet und entsprechend gehandhabt werden.

Ausgaben von Systemen, die als sensibel oder betriebswichtig eingestufte Informationen enthalten, sollten eine entsprechende Klassifizierungskennzeichnung tragen.

Weitere Informationen

Die Kennzeichnung klassifizierter Informationen stellt eine wesentliche Voraussetzung für die gemeinsame Nutzung dar.

Weitere nützliche Metadaten, die den Informationen beigefügt werden können, sind der organisatorische Prozess, der die Informationen erstellt hat, und der Zeitpunkt.

Die Kennzeichnung von Informationen und anderer zugehöriger Werte kann unter Umständen negative Auswirkungen haben. Klassifizierte Werte können von böswilligen Akteuren leichter identifiziert und missbraucht werden.

Einige Systeme kennzeichnen einzelne Dateien oder Datenbankeinträge nicht mit ihrer Klassifizierung, sondern schützen alle Informationen auf der höchsten Klassifizierungsstufe der Informationen, die sie enthalten oder enthalten dürfen. In solchen Systemen ist es üblich, Informationen zu ermitteln und dann beim Export zu kennzeichnen.

5.14 Informationsübertragung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Schutz

Maßnahme

Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien sollten Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.

Zweck

Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen interessierten Partei, ist aufrechterhalten.

Leitfaden

Allgemeines

Die Organisation sollte eine themenspezifische Richtlinie für die Übertragung von Informationen aufstellen und sie allen relevanten interessierten Parteien mitteilen. Die Regeln, Verfahren und Vereinbarungen zum Schutz von Informationen bei der Übertragung sollten der Klassifizierung der betreffenden Informationen entsprechen. Wenn Informationen zwischen der Organisation und Dritten übertragen werden, sollten Übertragungsvereinbarungen (einschließlich der Authentifizierung des Empfängers) getroffen und aufrechterhalten werden, um Informationen in jeder Form während der Übertragung zu schützen (siehe 5.10).

Die Informationsübertragung kann durch elektronische Übertragung, physische Speichermedien und mündliche Übermittlung erfolgen.

Für alle Arten der Informationsübertragung sollten Regeln, Verfahren und Vereinbarungen gelten:

- a) Maßnahmen zum Schutz der übertragenen Informationen vor Abfangen, unbefugtem Zugriff, Vervielfältigung, Änderung, Fehlleitung, Zerstörung und Dienstverweigerung, einschließlich einer der Klassifizierung der betreffenden Informationen entsprechenden Zugangssteuerung und spezieller Maßnahmen, die zum Schutz sensibler Informationen erforderlich sind, wie z. B. die Verwendung kryptographischer Techniken (siehe 8.24);
- b) Maßnahmen zur Sicherstellung der Rückverfolgbarkeit und Nichtabstreitbarkeit einschließlich der Einhaltung einer Kontrollkette für Informationen, die transferiert werden;
- c) Identifizierung geeigneter Kontaktpersonen für die Übertragung, einschließlich der Verantwortlichen der Informationen, der Risikoverantwortlichen, der Sicherheitsbeauftragten und der Informationsverwalter, soweit zutreffend;
- d) Verantwortlichkeiten und Haftung bei Informationssicherheitsvorfällen wie Verlust physischer Speichermedien oder Daten;
- e) 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 5.13);
- f) Zuverlässigkeit und Verfügbarkeit des Übertragungsdienstes;
- g) die themenspezifische Richtlinie oder die Leitlinien für die zulässige Nutzung von Einrichtungen zur Informationsübertragung (siehe 5.10);
- h) Aufbewahrungs- und Entsorgungsleitlinien für alle Geschäftsunterlagen, einschließlich Nachrichten;

ANMERKUNG Für die Aufbewahrung und Entsorgung von Geschäftsunterlagen können örtliche Gesetze und Vorschriften bestehen.

- i) die Berücksichtigung sonstiger einschlägiger rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen (siehe 5.31, 5.32, 5.33, 5.34) im Zusammenhang mit der Übertragung von Informationen (z. B. Anforderungen an elektronische Signaturen).

Elektronische Übertragung

In den Regeln, Verfahren und Vereinbarungen sollten auch die folgenden Punkte berücksichtigt werden, wenn elektronische Kommunikationsmittel für die Informationsübertragung genutzt werden:

- a) Erkennung von und zum Schutz vor Schadsoftware, die durch die Verwendung elektronischer Kommunikationseinrichtungen übertragen werden können (siehe 8.7);
- b) Schutz übertragener sensibler elektronischer Informationen, die in Form eines Anhangs vorliegen;
- c) Vorbeugung gegen die Versendung von Dokumenten und Nachrichten in Mitteilungen an eine falsche Adresse oder Nummer;
- d) Einholung einer Genehmigung vor der Nutzung externer öffentlicher Dienste wie Instant Messaging, soziale Netzwerke, Dateiaustausch oder Cloud-Speicherung;
- e) stärkere Authentifizierungsstufen bei der Übertragung von Informationen über öffentlich zugängliche Netze;
- f) Beschränkungen in Verbindung mit elektronischen Kommunikationseinrichtungen (z. B. automatische Weiterleitung von E-Mails an externe E-Mail-Adressen);
- g) Anweisung an das Personal und andere interessierte Parteien, keine Kurznachrichten (SMS) oder Sofortnachrichten mit kritischen Informationen zu versenden, da diese an öffentlichen Orten (und damit von Unbefugten) gelesen oder in nicht ausreichend geschützten Geräten gespeichert werden können;
- h) Anweisung an das Personal und andere interessierte Parteien bezüglich der Probleme bei der Nutzung von Faxgeräten oder -diensten, nämlich:
 - 1) unbefugter Zugriff auf eingebaute Nachrichtenspeicher zum Abruf von Nachrichten;
 - 2) vorsätzliche oder unbeabsichtigte Programmierung der Maschinen, so dass diese Nachrichten an bestimmte Nummern senden.

Übertragung physischer Speichermedien

Bei der Übertragung von physischen Speichermedien (einschließlich Papier) sollten die Regeln, Verfahren und Vereinbarungen auch Folgendes umfassen:

- a) Verantwortlichkeiten zur Steuerung von und zur Mitteilung bezüglich Übertragung, Versand und Empfang;
- b) Sicherstellung der korrekten Adressierung und Beförderung der Nachricht;
- c) eine Verpackung, die den Inhalt vor physischen Schäden schützt, zu denen es während des Transports kommen kann, und den Spezifikationen des Herstellers entspricht, zum Beispiel Schutz vor Umwelteinflüssen, die die Wirksamkeit der Wiederherstellung von Speichermedien beeinträchtigen können, wie z. B. Hitze, Feuchtigkeit oder elektromagnetische Felder; Anwendung technischer Mindestnormen für Verpackung und Versand (z. B. Verwendung undurchsichtiger Umschläge);
- d) eine Liste befugter zuverlässiger Kurier, die von der Geschäftsleitung genehmigt wurde;
- e) Standards zur Identifizierung eines Kurierunternehmens;
- f) je nach Klassifizierungsgrad der Informationen in den zu transportierenden Speichermedien manipulationssichere oder manipulationssichere Kontrollen (z. B. Taschen, Behälter) verwenden;

- g) Verfahren zur Verifizierung der Identität der Kuriere;
- h) genehmigte Liste von Dritten, die Transport- oder Kurierdienste anbieten, je nach Klassifizierung der Informationen;
- i) Führung von Protokollen zur Identifizierung des Inhalts der Speichermedien, des angewandten Schutzes sowie zur Aufzeichnung der Liste der berechtigten Empfänger, der Zeitpunkte der Übergabe an die Transportwächter und die Entgegennahme am Bestimmungsort.

Mündliche Übertragung

Um die mündliche Übertragung von Informationen zu schützen, sollten das Personal und andere interessierte Parteien daran erinnert werden, dass sie Folgendes tun sollten:

- a) keine vertraulichen mündlichen Gespräche an öffentlichen Orten oder über unsichere Kommunikationskanäle führen, da diese von Unbefugten abgehört werden können;
- b) kein Hinterlassen von vertraulichen Informationen enthaltenden Mitteilungen auf Anrufbeantwortern oder Sprachnachrichten, da diese beim Wählen einer falschen Nummer von unbefugten Personen wiedergegeben oder auf öffentlichen Systemen bzw. nicht ordnungsgemäß gespeichert werden können;
- c) auf die richtige Lautstärke eingestellt werden, um das Gespräch mitzuhören;
- d) sicherstellen, dass geeignete Maßnahmen zur Raumüberwachung getroffen werden (z. B. Schalldämmung, geschlossene Türen);
- e) alle sensiblen Gespräche sollten mit einer Erklärung beginnen, damit die Anwesenden wissen, welche Klassifizierungsstufe und welche Anforderungen an den Umgang mit dem, was sie hören werden, gestellt werden.

Weitere Informationen

Keine weiteren Informationen.

5.15 Zugangssteuerung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte sollten auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.

Zweck

Sicherstellung des befugten Zugangs und Verhinderung des unbefugten Zugangs auf Informationen und andere zugehörige Werte.

Leitfaden

Die Zuständigen von Informationen und anderen zugehörigen Werten sollten die Anforderungen an die Informationssicherheit und das Geschäft in Bezug auf die Zugangssteuerung festlegen. Eine themenspezifische Richtlinie zur Zugangssteuerung sollte festgelegt werden, die diesen Anforderungen Rechnung trägt und allen relevanten interessierten Parteien mitgeteilt werden sollte.

Bei diesen Anforderungen und der themenspezifischen Richtlinie sollte Folgendes berücksichtigt werden:

- a) Festlegung, welche Entitäten welche Art von Zugang zu den Informationen und anderen zugehörigen Werten benötigen;
- b) Sicherheit der Anwendungen (siehe 8.26);
- c) physischer Zugang, der durch geeignete physische Zugangskontrollen unterstützt werden muss (siehe 7.2, 7.3, 7.4);
- d) Verteilung und Genehmigung von Informationen (z. B. der Grundsatz „Kenntnis nur wenn erforderlich“), Informationssicherheitsstufen und Klassifizierung von Informationen (siehe 5.10, 5.12, 5.13);
- e) Einschränkungen des privilegierten Zugriffs (siehe 8.2);
- f) Aufgabentrennung (siehe 5.3);
- g) relevante Gesetzgebung, Vorschriften und vertragliche Verpflichtungen hinsichtlich der Begrenzung des Zugangs auf Daten oder Dienstleistungen (siehe 5.31, 5.32, 5.33, 5.34, 8.3);
- h) Trennung von Zugangssteuerungsfunktionen (z. B. Zugangsbeantragung, Zugangsgenehmigung, Zugangsverwaltung);
- i) offizielle Genehmigung von Zugangsbeantragungen (siehe 5.16 und 5.18);
- j) das Management von Zugangsrechten (siehe 5.18);
- k) Protokollierung (siehe 8.15).

Zugriffskontrollregeln sollten durch die Definition und Zuordnung geeigneter Zugriffsrechte und -beschränkungen zu den relevanten Entitäten umgesetzt werden (siehe 5.16). Eine Entität kann sowohl einen menschlichen Benutzer als auch ein technisches oder logisches Objekt (z. B. eine Maschine, ein Gerät oder einen Dienst) darstellen. Um das Management der Zugangssteuerung zu vereinfachen, können Entitätsgruppen bestimmte Rollen zugewiesen werden.

Bei der Festlegung und Umsetzung von Zugangssteuerungsregeln sollte Folgendes berücksichtigt werden:

- a) Konsistenz zwischen den Zugangsberechtigungen und der Informationsklassifizierung;
- b) Konsistenz zwischen den Zugangsberechtigungen und Anforderungen an die Sicherheit des physischen Perimeters;
- c) Berücksichtigung aller Arten von verfügbaren Verbindungen in verteilten Umgebungen, so dass Entitäten nur Zugang zu Informationen und anderen zugehörigen Ressourcen, einschließlich Netzwerken und Netzwerkdiensten, erhalten, zu deren Nutzung sie berechtigt sind;
- d) Überlegungen, wie Elemente oder Faktoren, die für die dynamische Zugangssteuerung relevant sind, berücksichtigt werden können.

Weitere Informationen

Im Zusammenhang mit der Zugangssteuerung werden häufig übergreifende Grundsätze verwendet. Zwei der am häufigsten verwendeten Grundsätze sind:

- a) Kenntnis nur wenn nötig: eine Entität erhält nur Zugang zu Informationen, die sie für die Erfüllung ihrer Aufgaben benötigt (unterschiedliche Aufgaben oder Rollen bedeuten unterschiedliche Kennntnisanforderungen und damit unterschiedliche Zugangsprofile);
- b) Notwendigkeit der Nutzung: Eine Entität erhält nur dann Zugang zur informationstechnischen Infrastruktur, wenn ein eindeutiger Bedarf besteht.

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

- a) Festlegen von Regeln auf Grundlage der Prämisse des geringsten Privilegs, „Es ist grundsätzlich alles verboten ist, was nicht ausdrücklich gestattet wird“ anstatt der schwächeren Regel „Grundsätzlich ist alles erlaubt, sofern es nicht ausdrücklich verboten ist“;
- b) Änderungen bei der Kennzeichnung von Informationen (siehe 5.13), die automatisch durch Einrichtungen zur Informationsverarbeitung und solche, die nach Ermessen eines Benutzers ausgelöst werden;
- c) Änderungen von Benutzerberechtigungen, die automatisch durch das Informationssystem und solche, die durch einen Administrator ausgelöst werden;
- d) Zeitpunkt, wann die Genehmigung festgelegt und regelmäßig überprüft werden soll.

Zugangssteuerungsregeln sollten durch dokumentierte Verfahrensweisen (siehe 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) und festgelegte Verantwortlichkeiten (siehe 5.2, 5.17) unterstützt werden.

Es gibt verschiedene Möglichkeiten der Zugangssteuerung, wie MAC (systembestimmte Zugriffskontrolle), DAC (benutzerbestimmbare Zugriffskontrolle, RBAC (rollenbasierte Zugriffskontrolle) und ABAC (attributbasierte Zugangssteuerung).

Zugangssteuerungsregeln können auch dynamische Elemente enthalten (z. B. eine Funktion, die vergangene Zugänge oder bestimmte Umgebungswerte auswertet). Zugangssteuerungsregeln können in unterschiedlicher Granularität implementiert werden, von der Abdeckung ganzer Netze oder Systeme bis hin zu spezifischen Datenfeldern, und können auch Eigenschaften wie den Standort des Benutzers oder die Art der Netzwerkverbindung, die für den Zugang verwendet wird, berücksichtigen. Diese Grundsätze und die Art und Weise, wie die granulare Zugangssteuerung definiert wird, können erhebliche Auswirkungen auf die Kosten haben. Strengere Regeln und mehr Granularität führen in der Regel zu höheren Kosten. Anhand von Geschäftsanforderungen und Risikoerwägungen sollte festgelegt werden, welche Zugangssteuerungsregeln angewendet werden und welche Granularität erforderlich ist.

5.16 Identitätsmanagement

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Der gesamte Lebenszyklus von Identitäten sollte verwaltet werden.

Zweck

Ermöglichung der eindeutigen Identifizierung von Personen und Systemen, die auf die Informationen der Organisation und andere zugehörige Werte zugreifen, sowie der angemessenen Zuweisung von Zugangsrechten.

Leitfaden

Die im Rahmen des Identitätsmanagements eingesetzten Verfahren sollten Folgendes sicherstellen:

- bei Identitäten, die Personen zugeordnet sind, wird eine bestimmte Identität nur mit einer einzigen Person verknüpft, um die Person für Handlungen, die mit dieser bestimmten Identität durchgeführt wurden, zur Rechenschaft ziehen zu können;
- Identitäten, die mehreren Personen zugewiesen sind (z. B. geteilte Identitäten), sind nur zulässig, wenn sie aus geschäftlichen oder betrieblichen Gründen erforderlich sind, und unterliegen einer speziellen Genehmigung und Dokumentation;
- Identitäten, die nicht-menschlichen Entitäten zugewiesen werden, unterliegen einer angemessenen getrennten Genehmigung und einer unabhängigen laufenden Beaufsichtigung;
- Identitäten werden rechtzeitig deaktiviert oder entfernt, wenn sie nicht mehr benötigt werden (z. B. wenn die zugehörigen Entitäten gelöscht oder nicht mehr verwendet werden oder wenn die mit einer Identität verknüpfte Person die Organisation verlassen oder die Rolle gewechselt hat);
- in einer bestimmten Domäne wird eine einzige Identität einer einzigen Entität zugeordnet, [d. h. die Zuordnung mehrerer Identitäten zu derselben Entität innerhalb desselben Kontexts (doppelte Identitäten) wird vermieden];
- Aufzeichnungen aller signifikanten Ereignisse, die die Nutzung und Verwaltung von Benutzeridentitäten sowie Authentisierungsinformationen betreffen, werden geführt.

Die Organisation sollte über einen unterstützenden Prozess verfügen, um Änderungen an Informationen im Zusammenhang mit Benutzeridentitäten zu handhaben. Diese Prozesse können eine erneute Überprüfung von vertrauenswürdigen Dokumenten zu einer Person beinhalten.

Bei der Verwendung von Identitäten, die von Dritten bereitgestellt oder ausgestellt werden (z. B. Zugangsdaten für soziale Medien), sollte die Organisation sicherstellen, dass die Identitäten Dritter das erforderliche Vertrauensniveau bieten und alle damit verbundenen Risiken bekannt sind und ausreichend behandelt werden. Dies kann sowohl Maßnahmen in Bezug auf Dritte (siehe 5.19) als auch Maßnahmen in Bezug auf die zugehörigen Authentifizierungsinformationen (siehe 5.17) umfassen.

Weitere Informationen

Die Gewährung bzw. der Entzug des Zugangs zu Informationen oder anderer zugehöriger Werte erfolgt üblicherweise im Rahmen eines mehrstufigen Verfahrens:

- die Bestätigung der geschäftlichen Anforderungen für eine zu erstellende Identität;
- Überprüfung der Identität einer Entität, bevor ihr eine logische Identität zugewiesen wird;
- Feststellung einer Identität;
- Konfigurieren und Aktivieren der Identität. Dazu gehört auch die Konfiguration und Ersteinrichtung der entsprechenden Authentifizierungsdienste;
- Gewährung oder Entzug bestimmter Zugangsrechte zur Identität auf der Grundlage entsprechender Autorisierungs- oder Berechtigungsentscheidungen (siehe 5.18).

5.17 Informationen zur Authentifizierung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Die Zuweisung und Verwaltung von Authentifizierungsinformationen sollte durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.

Zweck

Zur Sicherstellung einer ordnungsgemäßen Authentifizierung von Unternehmen und zur Vermeidung von Fehlern bei Authentifizierungsprozessen.

Leitfaden

Zuweisung von Authentifizierungsinformationen

Der Zuweisungs- und Managementprozess sollte sicherstellen, dass:

- persönliche Kennwörter oder persönliche Identifikationsnummern (PINs), die automatisch während des Anmeldevorgangs als vorübergehende geheime Authentifizierungsinformationen generiert werden, nicht erraten werden können und für jede Person einzigartig sind, und dass die Benutzer verpflichtet sind, sie nach der ersten Verwendung zu ändern;

- b) Verfahren eingerichtet werden, mit denen die Identität eines Benutzers vor der Zustellung neuer, die bisherigen ersetzende oder temporär gültiger geheimer Authentisierungsinformationen überprüft werden kann;
- c) Authentifizierungsinformationen, einschließlich vorübergehender Authentifizierungsinformationen, den Benutzern auf sichere Weise (z. B. über einen authentifizierten und geschützten Kanal) übermittelt werden, und die Verwendung ungeschützter (Klartext-)E-Mail-Nachrichten zu diesem Zweck vermieden wird;
- d) Benutzer den Erhalt von Authentisierungsinformationen bestätigen;
- e) die vordefinierten oder von den Anbietern bereitgestellten Standard-Authentifizierungsinformationen unmittelbar nach der Installation von Systemen oder Software geändert werden;
- f) Aufzeichnungen über wichtige Ereignisse im Zusammenhang mit der Zuweisung und Verwaltung von Authentifizierungsdaten geführt werden und ihre Vertraulichkeit gewährleistet ist und dass das Verfahren zur Aufbewahrung der Aufzeichnungen genehmigt ist (z. B. durch Verwendung eines genehmigten Kennwort-Tresor-Tools).

Benutzerverantwortlichkeiten

Jede Person, die Zugang zu Authentifizierungsdaten hat oder diese verwendet, sollte auf folgende Punkte hingewiesen werden:

- a) geheime Authentifizierungsinformationen wie Kennwörter werden vertraulich behandelt. Persönliche, geheime Authentifizierungsdaten dürfen an niemanden weitergegeben werden. Geheime Authentifizierungsinformationen, die im Zusammenhang mit Identitäten verwendet werden, die mit mehreren Benutzern oder mit nicht-personenbezogenen Entitäten verknüpft sind, werden ausschließlich mit autorisierten Personen geteilt;
- b) betroffene oder kompromittierte Authentifizierungsdaten werden sofort geändert, sobald eine Kompromittierung bekannt wird oder ein anderer Hinweis darauf vorliegt;
- c) falls Kennwörter zur Authentifizierung verwendet werden, werden sichere Kennwörter nach den Empfehlungen für bewährte Verfahren gewählt, zum Beispiel:
 - 1) Kennwörter basieren auf keinem Sachverhalten, die eine andere Person unter Zuhilfenahme personenbezogener Daten (z. B. Namen, Telefonnummern, Geburtstage) einfach erraten oder erschließen kann;
 - 2) Kennwörter basieren nicht auf Wörterbucheinträgen oder deren Kombinationen;
 - 3) leicht zu merkende Passphrasen werden verwendet, und es sollten möglichst alphanumerische Zeichen und Sonderzeichen enthalten sein;
 - 4) Kennwörter haben eine Mindestlänge;
- d) die gleichen Kennwörter werden nicht für verschiedene Dienste und Systeme verwendet;
- e) die Verpflichtung zur Einhaltung dieser Regeln ist auch in den Beschäftigungs- und Vertragsbedingungen enthalten (siehe 6.2).

System zur Verwaltung von Kennwörtern

Wenn Kennwörter als Authentifizierungsinformationen verwendet werden, sollte das Kennwortmanagementsystem:

- a) den Benutzern die Möglichkeit bieten, eigene Kennwörter zu wählen und diese zu ändern sowie ein Bestätigungsverfahren beinhalten, das Eingabefehler abfängt;
- b) sichere Kennwörter nach den Empfehlungen für bewährte Verfahren [siehe c) unter „Benutzerverantwortlichkeiten“] durchsetzen;
- c) die Benutzer auffordern, ihr Kennwort bei der ersten Anmeldung zu ändern;
- d) die Änderung von Kennwörtern bei Bedarf durchsetzen, z. B. nach einem Sicherheitsvorfall oder bei Beendigung oder Wechsel des Arbeitsverhältnisses, wenn ein Benutzer über bekannte Kennwörter für Identitäten verfügt, die weiterhin aktiv sind (z. B. gemeinsam genutzte Identitäten);
- e) die Wiederverwendung früherer Kennwörter verhindern;
- f) die Verwendung von häufig verwendeten Kennwörtern und kompromittierten Benutzernamen sowie Kennwortkombinationen aus gehackten Systemen verhindern;
- g) Kennwörter bei der Eingabe nicht auf dem Bildschirm anzeigen;
- h) Kennwörter verschlüsselt speichern und übertragen.

Die Verschlüsselung und das Hashing von Kennwörtern sollten nach anerkannten kryptographischen Verfahren für Kennwörter durchgeführt werden (siehe 8.24).

Weitere Informationen

Kennwörter oder Passphrasen sind eine allgemein gebräuchliche Art von Authentisierungsinformation und ein übliches Mittel zur Verifizierung der Identität eines Benutzers. Andere Arten von Authentisierungsinformation sind kryptographische Schlüssel, auf Hardware-Token (z. B. Smartcards) gespeicherte Daten, die AuthentifizierungsCodes und biometrische Datenerzeuger wie Iris-Scans oder Fingerabdrücke erzeugen. Zusätzliche Informationen sind in der Normenreihe ISO/IEC 24760 zu finden.

Die häufige Änderung von Kennwörtern kann problematisch sein, da die Benutzer durch die häufigen Änderungen genervt sein, neue Kennwörter vergessen, sie an unsicheren Orten notieren oder unsichere Kennwörter wählen können. Durch die Bereitstellung von Single Sign On (SSO) oder anderer Authentifizierungsmanagement-Tools (z. B. Kennwort-Tresore) verringert sich die Menge der Authentifizierungsinformationen, die die Benutzer schützen müssen, und kann somit die Wirksamkeit dieser Maßnahme steigern. Allerdings kann sich bei Verwendung dieser Tools die Offenlegung von Authentifizierungsinformationen auch schwerwiegender auswirken.

Bei einigen Anwendungen müssen die Benutzerkennwörter von einer unabhängigen Stelle vergeben werden. In diesen Fällen gelten die Buchstaben a), c) und d) des „Systems zur Verwaltung von Kennwörtern“ nicht.

5.18 Zugangsrechte

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Zugangsrechte zu Informationen und anderen zugehörigen Werten sollten in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.

Zweck

Sicherstellen, dass der Zugang zu Informationen und anderen zugehörigen Werten entsprechend den Geschäftsanforderungen definiert und autorisiert ist.

Leitfaden

Erteilung und Entzug von Zugangsrechten

Der Bereitstellungsprozess für die Zuweisung bzw. Entziehung von physischen und logischen Zugangsrechten, die der authentifizierten Identität einer Entität gewährt werden, sollte folgende Punkte umfassen:

- Einholung der Genehmigung vom Zuständigen der Informationen und anderer zugehöriger Werte für die Nutzung der Informationen und anderer zugehöriger Werte (siehe 5.9). Auch eine gesonderte Genehmigung der Zugangsrechte durch das Management kann sinnvoll sein;
- unter Berücksichtigung der geschäftlichen Anforderungen und der themenspezifischen Richtlinien und Regeln der Organisation zur Zugangssteuerung;
- Berücksichtigung der Aufgabentrennung, einschließlich der Trennung der Rollen für die Genehmigung und die Umsetzung der Zugangsrechte und der Trennung von sich widersprechenden Rollen;
- Sicherstellung, dass Zugangsrechte entfernt werden, wenn jemand keinen Zugang zu den Informationen und anderen zugehörigen Werten benötigt, und insbesondere, dass Zugangsrechte von Benutzern, die die Organisation verlassen haben, rechtzeitig entfernt werden;
- Erwägung der Erteilung von zeitlich begrenzten Zugangsrechten und deren Entzug zum Ablaufdatum, insbesondere für zeitlich befristetes Personal oder zeitlich begrenzten Zugang, der vom Personal benötigt wird;
- überprüfen, dass die gewährte Berechtigungsstufe mit den themenspezifischen Richtlinien zur Zugangssteuerung (siehe 5.15) übereinstimmt und mit anderen Informationssicherheitsanforderungen wie der Aufgabentrennung (siehe 5.3) vereinbar ist;
- Sicherstellung, dass die Zugangsrechte (z. B. durch die Dienstleister) erst nach erfolgreichem Abschluss der Genehmigungsverfahren aktiviert werden;

- h) Aufrechterhalten eines zentralen Verzeichnisses der unter einer Benutzerkennung (ID, logisch oder physisch) gewährten Rechte für den Zugang zu Informationen und anderen zugehörigen Werten;
- i) Änderung der Zugangsrechte von Benutzern, die ihre Rolle oder ihren Arbeitsplatz gewechselt haben;
- j) die Entziehung oder Anpassung der physischen und logischen Zugangsrechte, was mittels Entfernung, Sperrung oder Ersetzung von Schlüsseln, Authentifizierungsinformationen, Ausweiskarten oder Abonnements erfolgen kann;
- k) Führung eines Verzeichnisses der Änderungen der logischen und physischen Zugangsrechte der Benutzer.

Überprüfung von Zugangsrechten

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

- a) die Benutzerzugangsrechte nach einem Wechsel innerhalb derselben Organisation (z. B. Stellenwechsel, Beförderung, Herabstufung) oder nach Beendigung des Arbeitsverhältnisses (siehe 6.1 bis 6.5);
- b) Genehmigungen von privilegierten Zugangsrechten.

Überlegungen vor dem Wechsel oder der Beendigung des Arbeitsverhältnisses

Die Zugangsrechte eines Benutzers zu Informationen und anderen zugehörigen Werten sollten vor jeder Änderung oder Beendigung des Beschäftigungsverhältnisses auf der Grundlage der Bewertung von z. B. folgenden Risikofaktoren überprüft und angepasst oder entfernt werden:

- a) die Frage, ob die Beendigung oder Änderung vom Benutzer oder vom Management ausgeht, sowie die Gründe für die Beendigung;
- b) die aktuellen Zuständigkeiten des Benutzers;
- c) Einstufung der derzeit zugänglichen Werte.

Weitere Informationen

Es sollte überlegt werden, auf der Grundlage von Geschäftsanforderungen Benutzerzugangsrollen einzurichten, welche eine Anzahl von Zugangsrechten zu typischen Benutzerzugangsprofilen zusammenfassen. Zugangsbeantragungen und -überprüfungen von Zugangsrechten lassen sich auf der Ebene derartiger Benutzerzugangsrollen einfacher handhaben als auf der Ebene von einzelnen Zugangsrechten.

Es sollte überlegt werden, Klauseln in Anstellungs- und Dienstleistungsverträge aufzunehmen, in denen Sanktionen für den Fall spezifiziert werden, dass ein unbefugter Zugang durch einen Beschäftigten versucht wird (siehe 5.20, 6.2, 6.4, 6.6).

Bei einer vom Management ausgehenden Beendigung des Arbeits- oder Vertragsverhältnisses kann es dazu kommen, dass darüber verärgertes Personal oder sonstige Benutzer, die zu externen Parteien gehören, 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.

Das Klonen ist ein effizientes Verfahren für Unternehmen, um Benutzern Zugang zu gewähren. Dies sollte jedoch sorgfältig auf der Grundlage der von der Organisation festgelegten Rollen erfolgen, anstatt einfach eine Identität mit allen zugehörigen Zugangsrechten zu klonen. Das Klonen birgt die Gefahr in sich, dass es zu übermäßigen Zugangsrechten zu Informationen und anderen damit verbundenen Werten führt.

5.19 Informationssicherheit in Lieferantenbeziehungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lieferantenbeziehungen	#Governance_und_Ökosystem #Schutz

Maßnahme

Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.

Zweck

Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Leitfaden

Die Organisation sollte eine themenspezifische Richtlinie für die Lieferantenbeziehungen aufstellen und sie allen relevanten interessierten Parteien mitteilen.

Die Organisation sollte Prozesse und Verfahren ermitteln und einführen, um Sicherheitsrisiken im Zusammenhang mit der Nutzung von Produkten und Dienstleistungen, die von Lieferanten bereitgestellt werden, zu begegnen. Dies sollte auch für die Nutzung von Ressourcen von Cloud-Anbietern durch die Organisation gelten. Zu diesen Prozessen und Verfahren sollten diejenigen gehören, die von der Organisation einzuführen sind, sowie diejenigen, die die Organisation vom Lieferanten für die Aufnahme der Nutzung der Produkte oder Dienstleistungen eines Lieferanten oder für die Beendigung der Nutzung der Produkte und Dienstleistungen eines Lieferanten verlangt, wie z. B.:

- Feststellung und Dokumentation der Arten von Lieferanten (z.B. IKT-Dienstleistungen, Logistik, Versorgungseinrichtungen, Finanzdienstleistungen, IKT-Infrastrukturkomponenten), die die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der Organisation beeinträchtigen können;
- die Festlegung, wie Lieferanten entsprechend der Sensibilität von Informationen, Produkten und Dienstleistungen zu bewerten und auszuwählen sind (z. B. durch Marktanalysen, Kundenreferenzen, Prüfung von Unterlagen, Beurteilungen vor Ort, Zertifizierungen);
- Bewertung und Auswahl von Produkten oder Dienstleistungen von Lieferanten, die über angemessene Informationssicherheitskontrollen verfügen, und deren Überprüfung; insbesondere die Genauigkeit und Vollständigkeit der vom Lieferanten implementierten Maßnahmen, die die Integrität der Informationen und der Informationsverarbeitung des Lieferanten und damit die Informationssicherheit der Organisation sicherstellen;
- Definition der Informationen, IKT-Dienste und der physischen Infrastruktur der Organisation, auf die Lieferanten zugreifen, sie überwachen, steuern oder nutzen können;
- Festlegung der Arten von IKT-Infrastrukturkomponenten und -dienstleistungen, die von Lieferanten bereitgestellt werden und die sich auf die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen der Organisation auswirken können;

- f) Beurteilung und Management der mit der Informationssicherheit verbundenen Risiken:
- 1) die Nutzung der Informationen der Organisation und anderer zugehöriger Werte durch die Lieferanten, einschließlich der Risiken, die von potentiell böswilligen Beschäftigten der Lieferanten ausgehen;
 - 2) Fehlfunktionen oder Schwachstellen der Produkte (einschließlich der in diesen Produkten verwendeten Softwarekomponenten und Unterkomponenten) oder der von den Lieferanten erbrachten Dienstleistungen;
- g) Überwachung der Einhaltung der festgelegten Anforderungen an die Informationssicherheit für jede Lieferanten- und Zugriffsart, einschließlich Überprüfung durch Dritte und Produktvalidierung;
- h) Abmilderung der Nichteinhaltung der Vorschriften durch einen Lieferanten, unabhängig davon, ob diese durch Überwachung oder auf andere Weise festgestellt wurde;
- i) Umgang mit Vorfällen und Gefahren im Zusammenhang mit Produkten und Dienstleistungen der Lieferanten einschließlich Verantwortlichkeiten sowohl der Organisation als auch der Lieferanten;
- j) Maßnahmen bezüglich Ausfallsicherheit sowie ggf. zur Wiederherstellung und für den Notfall, um die Verfügbarkeit der Informationen und der Informationsverarbeitung des Lieferanten und damit die Verfügbarkeit der Informationen der Organisation sicherzustellen;
- k) Sensibilisierung und Schulung für das Personal der Organisation, die Umgang mit Personal des Lieferanten haben, bezüglich der entsprechenden Beauftragungsrichtlinien und themenspezifischen Richtlinien, Prozessen und Verfahren sowie des richtigen Verhaltens je nach Art des Lieferanten und dessen Zugriffsbefugnis auf die Systeme und Informationen der Organisation;
- l) Management der erforderlichen Übertragung von Informationen, anderen zugehörigen Werten und allen anderen zu ändernden Daten sowie Sicherstellung, dass die Informationssicherheit während der gesamten Übertragungsphase gewahrt bleibt.
- m) Anforderungen zur Sicherstellung einer sicheren Beendigung der Lieferantenbeziehung, einschließlich:
- 1) Entziehung von Zugangsrechten;
 - 2) Verarbeitung von Informationen;
 - 3) Festlegung der Eigentumsrechte an dem während der Beauftragung entwickelten geistigen Eigentum;
 - 4) die Übertragbarkeit von Informationen im Falle eines Lieferantenwechsels oder Insourcing;
 - 6) Verwaltung der Aufzeichnungen;
 - 7) Rückgabe von Werten;
 - 8) sichere Entsorgung von Informationen und anderen zugehörigen Werten;
 - 9) laufende erforderliche Vertraulichkeitsbedingungen;
- n) Stufe der Personalsicherheit und der physischen Sicherheit, die vom Personal und den Einrichtungen des Lieferanten erwartet wird.

Die Verfahren für die Fortsetzung der Informationsverarbeitung für den Fall, dass der Lieferant nicht mehr in der Lage ist, seine Produkte oder Dienstleistungen bereitzustellen (z. B. aufgrund eines Vorfalls, weil der Lieferant nicht mehr im Geschäft ist oder einige Komponenten aufgrund technologischer Fortschritte nicht mehr anbietet), sollten in Betracht gezogen werden, um Verzögerungen bei der Beschaffung von Ersatzprodukten oder -dienstleistungen zu vermeiden (z. B. durch die vorherige Ermittlung eines alternativen Lieferanten oder die ständige Nutzung alternativer Lieferanten).

Weitere Informationen

In Fällen, in denen es einer Organisation nicht möglich ist, Anforderungen an einen Lieferanten zu stellen, sollte die Organisation:

- a) die in dieser Maßnahme gegebenen Hinweise bei der Entscheidung für einen Lieferanten und dessen Produkt oder Dienstleistung berücksichtigen;
- b) auf der Grundlage einer Risikobeurteilung gegebenenfalls Gegenmaßnahmen ergreifen.

Lieferanten mit einem unzureichenden Informationssicherheitsmanagement können die Vertraulichkeit von Informationen gefährden. Es sollten Maßnahmen festgelegt und angewendet werden, um den Zugang des Lieferanten zu Informationen und anderen zugehörigen Werten zu verwalten. So sollten beispielsweise Geheimhaltungsvereinbarungen geschlossen oder kryptographische Verfahren eingesetzt werden, wenn ein besonderes Bedürfnis besteht, die Informationen vertraulich zu halten. Ein weiteres Beispiel sind Risiken beim Schutz personenbezogener Daten, wenn die Lieferantenverträge den Transfer von bzw. den Zugriff auf Information über Ländergrenzen hinweg vorsieht. Der Organisation muss stets bewusst sein, dass ihr die rechtliche bzw. vertragliche Verantwortung für den Schutz der Informationen obliegt.

Risiken können auch durch unzureichende Maßnahmen der IKT-Infrastrukturkomponenten oder der von Lieferanten erbrachten Dienstleistungen verursacht werden. Fehlerhafte bzw. anfällige Komponenten oder Dienste können Verstöße gegen die Informationssicherheit in der Organisation oder bei einer anderen Entität verursachen (z. B. können sie eine Schadsoftware-Infektion, Angriffe oder andere Schäden bei anderen Entitäten als der Organisation verursachen).

Zu Einzelheiten siehe ISO/IEC 27036-2.

5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lieferantenbeziehungen	#Governance_und_Ökosystem #Schutz

Maßnahme

Je nach Art der Lieferantenbeziehung sollten die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.

Zweck

Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Leitfaden

Lieferantenvereinbarungen sollten festgelegt und dokumentiert werden, um sicherzustellen, dass ein klares Verständnis zwischen der Organisation und dem Lieferanten in Bezug auf die Verpflichtungen der beiden Parteien bezüglich der Erfüllung der relevanten Anforderungen an die Informationssicherheit besteht.

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

- a) Beschreibung der Informationen, die bereitgestellt oder auf die zugegriffen werden soll und Methoden für die Bereitstellung der/den Zugriff auf die Informationen;
- b) Klassifizierung von Informationen entsprechend dem Klassifizierungsschema der Organisation (siehe 5.10, 5.12, 5.13);
- c) Abgleich des eigenen Klassifizierungsschemas der Organisation mit jenem des Lieferanten;
- d) rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, einschließlich des Datenschutzes, des Umgangs mit personenbezogenen Daten (pD), der Rechte an geistigem Eigentum und des Urheberrechts, sowie eine Beschreibung, wie sichergestellt wird, dass sie erfüllt werden;
- e) Verpflichtung jeder Vertragspartei zur Umsetzung einer Reihe vereinbarter Maßnahmen, einschließlich Zugangssteuerung, Leistungsüberprüfung, Überwachung, Meldung und Auditierung, sowie die Verpflichtung des Lieferanten zur Einhaltung der Informationssicherheitsanforderungen der Organisation;
- f) Regeln zur zulässigen Nutzung sowie ggf. bezüglich der unzulässigen Nutzung von Informationen und anderen zugehörigen Werten;
- g) Verfahren oder Bedingungen für die Genehmigung und den Entzug der Genehmigung für die Nutzung der Informationen der Organisation und anderer zugehöriger Werte durch das Personal der Lieferanten (z. B. durch eine ausdrückliche Liste des Personals der Lieferanten, das zur Nutzung der Informationen der Organisation und anderer zugehöriger Werte berechtigt ist);
- h) Anforderungen an die Informationssicherheit in Bezug auf die IKT-Infrastruktur des Lieferanten; insbesondere Mindestanforderungen an die Informationssicherheit für jede Informations- und Zugriffsort als Grundlage für die einzelnen Lieferantenverträge entsprechend den geschäftlichen Bedürfnissen der Organisation sowie ihren Risikokriterien;
- i) Entschädigungen und Abhilfemaßnahmen bei Nichterfüllung der Anforderungen durch den Auftragnehmer;
- j) Anforderungen und Verfahren für die Handhabung von Vorfällen (insbesondere Benachrichtigung und Zusammenarbeit bei der Behebung von Vorfällen);
- k) Anforderungen bezüglich Schulung und Sensibilisierung für bestimmte Verfahren und Anforderungen an die Informationssicherheit (z. B. für die Reaktion auf Vorfälle, Berechtigungsverfahren);
- l) einschlägige Bestimmungen für die Vergabe von Unteraufträgen, einschließlich der durchzuführenden Maßnahmen, wie z. B. die Vereinbarung über die Inanspruchnahme von Unterauftragnehmern (z. B. die Forderung, dass diese den gleichen Verpflichtungen wie der Lieferant unterliegen, die Forderung, dass eine Liste der Unterauftragnehmer vorliegt, und die Forderung, dass diese vor jeder Änderung zu benachrichtigen sind);
- m) relevante Verträge, einschließlich einer Kontaktperson bei Fragen der Informationssicherheit;

- n) bestehende Überprüfungsanforderungen in Bezug auf die Beschäftigten des Lieferanten, sofern dies gesetzlich zulässig ist, einschließlich Verantwortlichkeiten für die Durchführung der Überprüfung und Benachrichtigungsverfahren, falls die Überprüfung nicht vollständig durchgeführt wurde oder das Ergebnis Anlass für Zweifel oder Bedenken gibt;
- o) die Nachweise und Bestätigungsmechanismen von Bescheinigungen Dritter für relevante Informationssicherheitsanforderungen in Bezug auf die Prozesse des Lieferanten und einen unabhängigen Bericht über die Wirksamkeit der Maßnahmen;
- p) Recht zur Überprüfung der Lieferantenprozesse und Maßnahmen im Zusammenhang mit dem Vertrag;
- q) Verpflichtung des Lieferanten, in regelmäßigen Abständen einen Bericht zur Wirksamkeit der Maßnahmen vorzulegen und Zusicherung, relevante Probleme zu beheben, die im Bericht erwähnt werden;
- r) Fehlerbehebungs- und Konfliktlösungsprozesse;
- s) Bereitstellung von Sicherungskopien, die auf die Bedürfnisse des Unternehmens abgestimmt sind (in Bezug auf Häufigkeit, Art und Speicherort);
- t) Sicherstellung der Verfügbarkeit einer alternativen Einrichtung (d.h. eines Standorts für die Wiederherstellung im Katastrophenfall), die nicht den gleichen Bedrohungen ausgesetzt ist wie die primäre Einrichtung, und Überlegungen zu Ausweichmaßnahmen (alternativen Maßnahmen) für den Fall, dass die primären Maßnahmen ausfallen;
- u) ein Änderungsmanagementprozess, der sicherstellt, dass die Organisation vorab informiert wird und die Möglichkeit hat, Änderungen nicht anzunehmen;
- v) physische Sicherheitsmaßnahmen, die der Klassifizierung der Informationen angemessen sind;
- w) Maßnahmen zur Informationsübertragung, um die Informationen während der physischen oder logischen Übertragung zu schützen;
- x) Kündigungsklauseln bei Beendigung der Vereinbarung, einschließlich der Verwaltung von Unterlagen, der Rückgabe von Vermögenswerten, der sicheren Entsorgung von Informationen und anderen zugehörigen Werten sowie aller laufenden Vertraulichkeitsverpflichtungen;
- y) Bereitstellung eines Verfahrens zur sicheren Vernichtung der vom Lieferanten gespeicherten Informationen der Organisation, sobald diese nicht mehr benötigt werden;
- z) bei Vertragsende Sicherstellung der Übergabe der Supportleistungen an einen anderen Anbieter oder an die Organisation selbst.

Die Organisation sollte ein Verzeichnis der Vereinbarungen mit externen Parteien (z. B. Verträge, Absichtserklärungen, Vereinbarungen über die gemeinsame Nutzung von Informationen) erstellen und führen, um den Überblick darüber zu behalten, wohin ihre Informationen gehen. Die Organisation sollte auch ihre Vereinbarungen mit externen Parteien regelmäßig überprüfen, validieren und aktualisieren, um sicherzustellen, dass sie weiterhin erforderlich und zweckdienlich sind und relevante Informationssicherheitsklauseln enthalten.

Weitere Informationen

Die Verträge verschiedener Organisationen mit verschiedenen Arten von Lieferanten können sich beträchtlich voneinander unterscheiden. Daher sollte sorgfältig darauf geachtet werden, alle relevanten Anforderungen für den Umgang mit Informationssicherheitsrisiken aufzuführen.

Einzelheiten zu Lieferantenvereinbarungen sind in der Normenreihe ISO/IEC 27036 zu finden. Für Vereinbarungen über Cloud-Dienste siehe die Normenreihe ISO/IEC 19086.

5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lieferantenbeziehungen	#Governance_und_Ökosystem #Schutz

Maßnahme

Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.

Zweck

Aufrechterhaltung eines vereinbarten Niveaus der Informationssicherheit in Lieferantenbeziehungen.

Leitfaden

Die folgenden Themen sollten berücksichtigt werden, um die Informationssicherheit innerhalb der IKT-Lieferkette zusätzlich zu den allgemeinen Anforderungen an die Informationssicherheit in den Lieferantenbeziehungen zu behandeln:

- Festlegung von Anforderungen an die Informationssicherheit, die für den Erwerb von IKT-Produkten oder -Dienstleistungen gelten;
- die Forderung, dass die Lieferanten von IKT-Dienstleistungen die Sicherheitsanforderungen der Organisation in der gesamten Lieferkette weitergeben, wenn sie Teile der für die Organisation erbrachten IKT-Dienstleistung untervergeben;
- die Verpflichtung der Anbieter von IKT-Produkten, geeignete Sicherheitspraktiken in der gesamten Lieferkette zu verbreiten, wenn diese Produkte Komponenten enthalten, die von anderen Anbietern oder anderen Stellen gekauft oder erworben wurden (z. B. Softwareentwickler und Anbieter von Hardwarekomponenten im Unterauftrag);
- Aufforderung an die Anbieter von IKT-Produkten, Informationen über die in den Produkten verwendeten Softwarekomponenten zu liefern;
- Aufforderung an die Anbieter von IKT-Produkten, Informationen über die implementierten Sicherheitsfunktionen ihres Produkts und die für den sicheren Betrieb erforderliche Konfiguration bereitzustellen;
- Umsetzung eines Überwachungsprozesses sowie geeigneter Methoden zur Sicherstellung, dass die bereitgestellten IKT-Produkte und -Dienstleistungen die festgelegten Sicherheitsanforderungen erfüllen. Beispiele für solche Überprüfungsverfahren des Anbieters können Penetrationstests und der Nachweis oder die Validierung von Bescheinigungen Dritter für die Informationssicherheitsmaßnahmen des Anbieters sein;

- g) Umsetzung eines Prozesses zur Festlegung und Dokumentation von Produkt- oder Dienstkomponenten, die zur Aufrechterhaltung der Funktion wesentlich sind und daher einer besonderen Aufmerksamkeit, Prüfung und weiterer Nachverfolgung bedürfen, wenn sie außerhalb der Organisation erstellt werden, insbesondere wenn der Lieferant bestimmte Aspekte der Produkt- oder Dienstkomponenten an andere Lieferanten untervergibt;
- h) Einholen der Zusicherung, dass kritische Komponenten und ihr Ursprung über die gesamte Lieferkette verfolgt werden können;
- i) Einholen der Zusicherung, dass die bereitgestellten IKT-Produkte wie erwartet funktionieren und keine unerwarteten oder unerwünschten Eigenschaften aufweisen;
- j) Umsetzung von Verfahren, mit denen sichergestellt wird, dass die von den Lieferanten gelieferten Komponenten echt sind und nicht von ihrer Spezifikation abweichen. Zu den Maßnahmen gehören beispielsweise Kennzeichnungen zum Schutz vor Manipulationen, kryptographische Hash-Verifizierungen oder digitale Signaturen. Die Überwachung auf Abweichungen von der Spezifikation kann ein Indikator für Manipulationen oder Fälschungen sein. Die Verhinderung und Erkennung von Manipulationen sollte in mehreren Phasen des Lebenszyklus der Systementwicklung erfolgen, einschließlich Gestaltung, Entwicklung, Integration, Betrieb und Wartung;
- k) Erlangung der Gewissheit, dass IKT-Produkte die geforderten Sicherheitsstufen erreichen, z. B. durch formale Zertifizierung oder ein Evaluierungssystem wie das Common Criteria Recognition Arrangement;
- l) Festlegung von Regeln für die Mitteilung von Informationen bezüglich der Lieferkette und möglicher Probleme und Kompromisse zwischen der Organisation und den Lieferanten;
- m) Umsetzung spezifischer Prozesse für das Management des Lebenszyklus und der Verfügbarkeit von IKT-Komponenten 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. Die Identifizierung eines alternativen Lieferanten und das Verfahren zur Übertragung von Software und Kompetenzen auf den alternativen Lieferanten sollten in Betracht gezogen werden.

Weitere Informationen

Die spezifischen Risikomanagementpraktiken für die IKT-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 IKT-Lieferkette sowie jedweder Angelegenheiten verfügen, die erhebliche Auswirkungen auf die bereitgestellten Produkte und Dienste haben. Die Organisation kann Einfluss auf die in der IKT-Lieferkette angewendeten Sicherheitspraktiken nehmen, indem sie in den Verträgen mit ihren Lieferanten deutlich machen, auf welche Aspekte die anderen Lieferanten innerhalb der IKT-Lieferkette eingehen sollten.

IKT sollten aus seriösen Quellen bezogen werden. Die Zuverlässigkeit von Software und Hardware ist eine Frage der Qualitätskontrolle. Auch wenn es einer Organisation im Allgemeinen nicht möglich ist, die Qualitätskontrollsysteme ihrer Lieferanten zu überprüfen, so kann sie doch auf der Grundlage des Rufs des Lieferanten ein zuverlässiges Urteil fällen.

Die hier behandelte IKT-Lieferkette umfasst auch Cloud-Dienste.

Beispiele für IKT-Lieferketten sind:

- a) die Bereitstellung von Cloud-Diensten, bei der der Anbieter von Cloud-Diensten auf die Software-Entwickler, Telekommunikationsdienstleister und Hardware-Anbieter angewiesen ist;

- b) IoT, wobei der Dienst die Gerätehersteller, die Anbieter von Cloud-Diensten (z. B. die Betreiber von IoT-Plattformen), die Entwickler von Mobil- und Webanwendungen und die Anbieter von Softwarebibliotheken einbezieht;
- c) Hosting-Dienste, bei denen der Anbieter auf externe Service-Desks einschließlich der ersten, zweiten und dritten Support-Ebene zurückgreift.

Weitere Einzelheiten, einschließlich einer Anleitung zur Risikobeurteilung, sind in ISO/IEC 27036-3 zu finden.

Software-Identifikationsetiketten (SWID) können auch zu einer besseren Informationssicherheit in der Lieferkette beitragen, indem sie Informationen über die Herkunft der Software liefern. Weitere Einzelheiten sind ISO/IEC 19770-2 zu entnehmen.

5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lieferantenbeziehungen #Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit	#Governance_und_Ökosystem #Schutz #Verteidigung

Maßnahme

Die Organisation sollte regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.

Zweck

Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung wird im Einklang mit Lieferantenverträgen aufrechterhalten.

Leitfaden

Durch die Überwachung, Überprüfung und das Änderungsmanagement von Lieferantenleistungen sollte sichergestellt werden, dass die Informationssicherheitsbedingungen der Vereinbarungen eingehalten werden, dass Vorfälle und Probleme im Bereich der Informationssicherheit ordnungsgemäß gehandhabt werden und dass Änderungen bei den Lieferantenleistungen oder dem Geschäftsstatus die Leistungserbringung nicht beeinträchtigen.

Dies sollte ein Verfahren zur Verwaltung der Beziehungen zwischen der Organisation und dem Lieferanten beinhalten:

- a) Überwachung der Dienstleistungserbringungsniveaus zur Verifizierung der Vertragserfüllung;
- b) die von den Lieferanten vorgenommenen Änderungen zu überwachen:
 - 1) Verbesserungen der derzeit bereitgestellten Dienstleistungen;
 - 2) Weiterentwicklungen jedweder neuer Anwendungen und Systeme;

- 3) Modifikationen oder Aktualisierungen in Bezug auf die Richtlinien und Verfahren des Lieferanten;
- 4) neue oder veränderte Maßnahmen zur Klärung von Informationssicherheitsvorfällen und zur Verbesserung der Informationssicherheit;
- c) Überwachung von Änderungen an den Lieferantendienstleistungen einschließlich:
 - 1) von Änderungen und Verbesserungen an den Netzwerken;
 - 2) zur Nutzung neuer Technologien;
 - 3) zur Einführung neuer Produkte oder neuerer Versionen oder Releases;
 - 4) neuer Entwicklungswerkzeuge und -umgebungen;
 - 5) von Änderungen am Standort der Dienstleistungseinrichtungen;
 - 6) von Unterlieferantenwechseln;
 - 7) von Untervertragsvergaben an andere Lieferanten;
- d) Überprüfung der vom Lieferanten vorgelegten Dienstleistungsberichte und Organisation der nach den Vereinbarungen erforderlichen, regelmäßigen Fortschrittsbesprechungen;
- e) Durchführung von Lieferanten- und Unterlieferanten-Audits in Verbindung mit der Überprüfung der ggf. verfügbaren Auditberichte sowie Nachverfolgung der festgestellten Probleme;
- f) Bereitstellung von Informationen zu Informationssicherheitsvorfällen und Überprüfung dieser Informationen entsprechend der vertraglichen Anforderungen sowie jedweder unterstützenden Richtlinien und Verfahren;
- g) Überprüfung der Lieferanten-Prüfpfade und der Aufzeichnungen zu Informationssicherheitsereignissen, betrieblichen Problemen, Ausfällen, Fehler-Nachverfolgungen und Unterbrechungen in Bezug auf die erbrachten Dienstleistungen;
- h) auf festgestellte Ereignisse oder Vorfälle im Bereich der Informationssicherheit zu reagieren und diese zu bewältigen;
- i) Schwachstellen in der Informationssicherheit zu erkennen und zu beheben;
- j) Überprüfung von Aspekten der Informationssicherheit bei den Beziehungen des Lieferanten zu seinen eigenen Lieferanten;
- k) 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 5.29, 5.30, 5.35, 5.36, 8.14) eingehalten wird;
- l) Sicherstellung, dass die Lieferanten Verantwortlichkeiten für die Überprüfung der Einhaltung und Durchsetzung der vertraglichen Anforderungen festlegen;
- m) regelmäßige Bewertung, ob die Lieferanten angemessene Informationssicherheitsstufen einhalten.

Die Verantwortung für das Management der Lieferantenbeziehungen sollte einer dazu eigens bestimmten Person oder einem Team übertragen werden. 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.

Weitere Informationen

Zu Einzelheiten siehe ISO/IEC 27036-3.

5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_in_Lieferantenbeziehungen	#Governance_und_Ökosystem #Schutz

Maßnahme

Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.

Zweck

Festlegung und Verwaltung der Informationssicherheit bei der Nutzung von Cloud-Diensten.

Leitfaden

Die Organisation sollte eine themenspezifische Richtlinie für die Nutzung von Cloud-Diensten aufstellen und sie allen relevanten interessierten Parteien mitteilen.

Die Organisation sollte festlegen und mitteilen, wie sie die mit der Nutzung von Cloud-Diensten verbundenen Informationssicherheitsrisiken zu handhaben gedenkt. Dies kann eine Erweiterung oder ein Teil des bestehenden Ansatzes sein, wie eine Organisation die von externen Parteien erbrachten Dienstleistungen verwaltet (siehe 5.21 und 5.22).

Die Nutzung von Cloud-Diensten kann eine gemeinsame Verantwortung für die Informationssicherheit und eine Zusammenarbeit zwischen dem Anbieter des Cloud-Dienstes und der Organisation, die als Kunde des Cloud-Dienstes auftritt, erfordern. Es ist von entscheidender Bedeutung, dass die Verantwortlichkeiten sowohl für den Cloud-Dienstleister als auch für die Organisation, die als Cloud-Dienstleistungskunde auftritt, angemessen definiert und umgesetzt werden.

Die Organisation sollte Folgendes festlegen:

- a) alle einschlägigen Anforderungen an die Informationssicherheit im Zusammenhang mit der Nutzung der Cloud-Dienste;
- b) Auswahlkriterien für Cloud-Dienste und Anwendungsbereich von Cloud-Diensten;
- c) Rollen und Verantwortlichkeiten im Zusammenhang mit der Nutzung und Verwaltung von Cloud-Diensten;

- d) welche Informationssicherheitsmaßnahmen vom Cloud-Dienstleister und welche von der Organisation als Cloud-Dienstleistungskunde verwaltet werden;
- e) wie man die vom Cloud-Dienstleister bereitgestellten Informationssicherheitsfunktionen erhält und nutzt;
- f) wie man sich Vertrauenswürdigkeit über die von den Cloud-Dienstleistern durchgeführten Maßnahmen zur Informationssicherheit verschaffen kann;
- g) wie Steuerungen, Schnittstellen und Änderungen von Diensten zu handhaben sind, wenn eine Organisation mehrere Cloud-Dienste nutzt, insbesondere von verschiedenen Cloud-Dienstleistern;
- h) Verfahren für den Umgang mit Informationssicherheitsvorfällen, die im Zusammenhang mit der Nutzung von Cloud-Diensten auftreten;
- i) ihren Ansatz zur Überwachung, Überprüfung und Bewertung der laufenden Nutzung von Cloud-Diensten, um Informationssicherheitsrisiken zu verwalten;
- j) wie die Nutzung von Cloud-Diensten geändert oder eingestellt werden kann, einschließlich Ausstiegsstrategien für Cloud-Dienste.

Cloud-Service-Vereinbarungen sind oft vordefiniert und können nicht verhandelt werden. Für alle Cloud-Dienste sollte die Organisation die Cloud-Dienstleistungsvereinbarungen mit dem/den Cloud-Dienstleister(n) überprüfen. Eine Cloud-Dienstleistungsvereinbarung sollte die Anforderungen der Organisation an Vertraulichkeit, Integrität, Verfügbarkeit und Informationsverarbeitung berücksichtigen und entsprechende Ziele für die Cloud-Dienstleistungsebene und die Qualität der Cloud-Dienste enthalten. Die Organisation sollte auch entsprechende Risikobeurteilungen durchführen, um die mit der Nutzung des Cloud-Dienstes verbundenen Risiken zu ermitteln. Etwaige Restrisiken, die mit der Nutzung des Cloud-Dienstes verbunden sind, sollten eindeutig identifiziert und von der zuständigen Leitung der Organisation angenommen werden.

Eine Vereinbarung zwischen dem Cloud-Dienstleister und der Organisation, die als Cloud-Dienstleistungskunde auftritt, sollte die folgenden Bestimmungen zum Schutz der Daten der Organisation und zur Verfügbarkeit der Dienste enthalten:

- a) Bereitstellung von Lösungen, die auf branchenweit anerkannten Normen für Architektur und Infrastruktur basieren;
- b) Verwaltung der Zugangssteuerungen des Cloud-Dienstes zur Erfüllung der Anforderungen des Unternehmens;
- c) Implementierung von Lösungen zur Überwachung und zum Schutz vor Schadsoftware;
- d) die Verarbeitung und Speicherung sensibler Informationen der Organisation an zugelassenen Orten (z. B. in einem bestimmten Land oder einer bestimmten Region) oder innerhalb einer bestimmten Gerichtsbarkeit oder unter einer bestimmten Gerichtsbarkeit;
- e) gezielte Unterstützung im Falle eines Informationssicherheitsvorfalls in der Cloud-Dienstumgebung;
- f) Sicherstellung, dass die Anforderungen der Organisation an die Informationssicherheit erfüllt werden, wenn Cloud-Dienste weiter an einen externen Dienstleister untervergeben werden (oder Verbot der Untervergabe von Cloud-Diensten);
- g) Unterstützung der Organisation bei der Sammlung digitaler Beweise unter Berücksichtigung der Gesetze und Vorschriften für digitale Beweise in den verschiedenen Rechtsordnungen;

- h) Bereitstellung eines angemessenen Supports und der Verfügbarkeit von Diensten für einen angemessenen Zeitraum, wenn das Unternehmen den Cloud-Dienst verlassen möchte;
- i) Bereitstellung der erforderlichen Sicherungskopien von Daten und Konfigurationsinformationen und ggf. sichere Verwaltung der Sicherungskopien auf der Grundlage der Fähigkeiten des von der Organisation als Cloud-Dienstleistungskunde genutzten Cloud-Dienstleisters;
- j) Bereitstellung und Rückgabe von Informationen wie Konfigurationsdateien, Quellcode und Daten, die Eigentum der Organisation sind, die als Cloud-Dienstleistungskunde auftritt, wenn sie während der Bereitstellung des Dienstes oder bei Beendigung des Dienstes angefordert werden.

Die Organisation, die als Cloud-Dienstleistungskunde auftritt, sollte berücksichtigen, ob die Vereinbarung vorsehen sollte, dass die Cloud-Dienstleister vor wesentlichen, sich auf den Kunden auswirkenden Änderungen an der Art und Weise, wie der Dienst für die Organisation erbracht wird, vorab informiert werden müssen:

- a) Änderungen an der technischen Infrastruktur (z. B. Umzug, Neukonfiguration oder Änderungen der Hardware oder Software), die sich auf das Cloud-Dienstleistungsangebot auswirken oder dieses verändern;
- b) Verarbeitung oder Speicherung von Informationen in einem neuen geographischen oder rechtlichen Zuständigkeitsbereich;
- c) die Nutzung von Peer-Cloud-Dienstleistern oder anderen Unterauftragnehmern (einschließlich des Wechsels bestehender oder des Einsatzes neuer Parteien).

Die Organisation, die Cloud-Dienste nutzt, sollte engen Kontakt zu ihren Cloud-Dienstleistern halten. Diese Kontakte ermöglichen den gegenseitigen Austausch von Informationen über die Informationssicherheit bei der Nutzung von Cloud-Diensten, einschließlich eines Mechanismus, mit dem sowohl der Cloud-Dienstleister als auch die Organisation, die als Cloud-Dienstleistungskunde auftritt, jedes Dienstmerkmal überwachen und Verstöße gegen die in den Vereinbarungen enthaltenen Verpflichtungen melden können.

Weitere Informationen

Bei dieser Maßnahme wird die Sicherheit der Cloud aus der Perspektive des Cloud-Dienstleistungskunden betrachtet.

Weitere Informationen zu Cloud-Diensten finden sich in ISO/IEC 17788, ISO/IEC 17789 und ISO/IEC 22123-1. Spezifische Angaben zur Cloud-Portabilität im Rahmen von Ausstiegsstrategien finden sich in ISO/IEC 19941. Spezifische Angaben zur Informationssicherheit und zu öffentlichen Cloud-Diensten sind in ISO/IEC 27017 beschrieben. Spezifische Angaben zum Schutz personenbezogener Daten in öffentlichen Clouds, die als Auftragsdatenverarbeiter fungieren, sind in ISO/IEC 27018 beschrieben. Die Lieferantenbeziehungen bei Cloud-Diensten werden von ISO/IEC 27036-4 abgedeckt, und die Vereinbarungen über Cloud-Dienste und ihr Inhalt werden in der Normenreihe ISO/IEC 19086 behandelt, wobei Sicherheit und Datenschutz speziell von ISO/IEC 19086-4 abgedeckt werden.

5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Governance #Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Die Organisation sollte die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.

Zweck

Sicherstellung einer schnellen, wirksamen, konsistenten und ordnungsgemäßen Reaktion auf Informationssicherheitsvorfälle, einschließlich der Kommunikation über Informationssicherheitsvorfälle.

Leitfaden

Rollen und Verantwortlichkeiten

Die Organisation sollte geeignete Prozesse für die Handhabung von Informationssicherheitsvorfällen einrichten. Die Rollen und Verantwortlichkeiten für die Durchführung der Verfahren zur Bewältigung von Vorfällen sollten festgelegt und den relevanten internen und externen interessierten Parteien wirksam mitgeteilt werden.

Folgendes sollte berücksichtigt werden:

- Einführung eines gemeinsamen Verfahrens für die Meldung von Informationssicherheitsvorfällen, einschließlich einer Kontaktstelle (siehe 6.8);
- Einrichtung eines Prozesses für das Management von Vorfällen, um die Organisation in die Lage zu versetzen, Vorfälle im Bereich der Informationssicherheit zu bewältigen, einschließlich Verwaltung, Dokumentation, Erkennung, Sichtung, Priorisierung, Analyse, Kommunikation und Koordinierung der beteiligten Parteien;
- Einrichtung eines Verfahrens zur Reaktion auf Vorfälle, um die Organisation in die Lage zu versetzen, Vorfälle im Bereich der Informationssicherheit zu beurteilen, auf sie zu reagieren und daraus zu lernen;
- nur kompetente Beschäftigte die Themen in Bezug auf Informationssicherheitsvorfälle innerhalb der Organisation bearbeiten lassen. Dieses Personal sollte eine Verfahrensdokumentation erhalten und regelmäßig geschult werden;
- Einführung eines Verfahrens zur Ermittlung der erforderlichen Ausbildung, Zertifizierung und ständigen beruflichen Weiterbildung für das Personal, das auf Vorfälle reagiert.

Verfahren für das Management von Vorfällen

Die Ziele der Handhabung von Informationssicherheitsvorfällen sollten mit der Leitung abgestimmt werden, und es sollte sichergestellt werden, dass die für die Handhabung von Informationssicherheitsvorfällen verantwortlichen Personen sich der Prioritäten der Organisation bei der Handhabung von Informationssicherheitsvorfällen bewusst sind einschließlich des Zeitrahmens für die Lösung des Problems auf der Grundlage der möglichen Folgen und des Schweregrads. Um diese Ziele und Prioritäten zu erreichen, sollten Verfahren für das Management von Vorfällen eingeführt werden.

Das Management sollte sicherstellen, dass ein Plan für die Handhabung von Informationssicherheitsvorfällen erstellt wird, der verschiedene Szenarien berücksichtigt, und dass Verfahren für die folgenden Aktivitäten entwickelt und umgesetzt werden:

- a) Bewertung von Ereignissen im Bereich der Informationssicherheit nach den Kriterien, die einen Vorfall im Bereich der Informationssicherheit darstellen;
- b) Überwachung (siehe 8.15 und 8.16), Erkennung (siehe 8.16), Klassifizierung (siehe 5.25), Analyse und Meldung (siehe 6.8) von Ereignissen und Vorfällen im Bereich der Informationssicherheit (durch menschliche oder automatische Mittel);
- c) Handhabung von Informationssicherheitsvorfällen bis zum Abschluss, einschließlich Reaktion und Eskalation (siehe 5.26), je nach Art und Kategorie des Vorfalls, mögliche Aktivierung des Krisenmanagements und Aktivierung von Plänen zur Aufrechterhaltung, kontrollierte Wiederherstellung nach einem Vorfall und Kommunikation mit internen und externen interessierten Parteien;
- d) Koordination mit internen und externen Interessenten wie Behörden, externen Interessengruppen und Foren, Lieferanten und Kunden (siehe 5.5 und 5.6);
- e) Protokollierung der Tätigkeiten bei der Handhabung von Vorfällen;
- f) Umgang mit Beweismitteln (siehe 5.28);
- g) Ursachenanalyse oder Post-Mortem-Verfahren;
- h) Ermittlung der gewonnenen Erkenntnisse und der erforderlichen Verbesserungen der Verfahren für das Management von Vorfällen oder der Maßnahmen für die Informationssicherheit im Allgemeinen.

Meldeverfahren

Meldeverfahren sollten beinhalten:

- a) Maßnahmen, die im Falle eines Informationssicherheitsereignisses zu ergreifen sind (z. B. unverzügliches Festhalten aller sachdienlichen Details wie auftretende Störungen und Meldungen auf dem Bildschirm, unverzügliche Meldung an die Kontaktstelle und nur koordinierte Maßnahmen);
- b) Verwendung von Formularen zur Unterstützung des Personals bei der Durchführung aller erforderlichen Maßnahmen zur Meldung von Informationssicherheitsvorfällen;
- c) geeignete Rückmeldungsprozesse, um sicherzustellen, dass Personen, die Informationssicherheitsereignisse gemeldet haben, soweit möglich über die Ergebnisse informiert werden, nachdem das Problem behandelt und abgeschlossen wurde;
- d) Erstellung von Vorfallsberichten.

Externe Anforderungen an die Meldung von Vorfällen an relevante interessierte Parteien innerhalb des festgelegten Zeitrahmens (z. B. Meldepflichten gegenüber Aufsichtsbehörden) sollten bei der Implementierung von Verfahren für die Handhabung von Vorfällen berücksichtigt werden.

Weitere Informationen

Informationssicherheitsvorfälle können Organisations- und Ländergrenzen überschreiten. Um auf derartige Vorfälle zu reagieren, ist es von Vorteil, die Reaktion zu koordinieren und Informationen über diese Vorfälle gegebenenfalls mit externen Organisationen auszutauschen.

Eine ausführliche Anleitung zur Handhabung von Informationssicherheitsvorfällen kann der Normenreihe ISO/IEC 27035 entnommen werden.

5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Die Organisation sollte Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden sollen.

Zweck

Sicherstellung einer effektiven Kategorisierung und Priorisierung von Informationssicherheitsereignissen.

Leitfaden

Es sollte ein Schema zur Kategorisierung und Priorisierung von Informationssicherheitsvorfällen vereinbart werden, um die Folgen und die Priorität eines Vorfalls zu ermitteln. Das System sollte die Kriterien für die Einstufung von Ereignissen als Informationssicherheitsvorfälle enthalten. Die Kontaktstelle sollte jedes Informationssicherheitsereignis anhand des vereinbarten Schemas beurteilen.

Das für die Koordinierung und Reaktion auf Informationssicherheitsvorfälle zuständige Personal sollte die Beurteilung durchführen und eine Entscheidung über Informationssicherheitsvorfälle treffen.

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

Weitere Informationen

Die Normenreihe ISO/IEC 27035 enthält weitere Anleitungen zur Handhabung von Vorfällen.

5.26 Reaktion auf Informationssicherheitsvorfälle

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Auf Informationssicherheitsvorfälle sollte entsprechend den dokumentierten Verfahren reagiert werden.

Zweck

Sicherstellung einer effizienten und wirksamen Reaktion auf Vorfälle im Bereich der Informationssicherheit.

Leitfaden

Die Organisation sollte Verfahren für die Reaktion auf Vorfälle im Bereich der Informationssicherheit einführen und allen betroffenen Parteien mitteilen.

Auf Informationssicherheitsvorfälle sollte von einem benannten Team mit der erforderlichen Kompetenz reagiert werden (siehe 5.24).

Die Reaktion sollte die folgenden Punkte umfassen:

- Eindämmen der von dem Vorfall betroffenen Systeme, wenn sich die Folgen des Vorfalls ausbreiten können;
- möglichst frühzeitiges Sichern von Beweismaterial (siehe 5.28) nach dem Vorkommnis;
- Eskalation, falls erforderlich, einschließlich Krisenmanagementaktivitäten und möglicherweise Inanspruchnahme von Betriebskontinuitätsplänen (siehe 5.29 und 5.30);
- Sicherstellung, dass alle durchgeführten Abhilfeaktivitäten zur späteren Analyse ordnungsgemäß protokolliert werden;
- Kommunikation des aufgetretenen Informationssicherheitsvorfalls bzw. jedweder relevanter Details an alle relevanten internen und externen interessierten Parteien nach dem Grundsatz „Kenntnis nur, wenn nötig“;
- Koordinierung mit internen und externen Parteien wie Behörden, externen Interessengruppen und Foren, Lieferanten und Kunden, um die Wirksamkeit der Maßnahmen zu verbessern und die Folgen für andere Organisationen zu minimieren;
- formeller Abschluss und Dokumentierung nach erfolgreicher Behandlung der Vorfallsbehandlung;
- Durchführung einer forensischen Informationssicherheitsanalyse, sofern erforderlich (siehe 5.28);
- Durchführung einer Analyse nach einem Vorfall, um die Ursache zu ermitteln. Es wird sichergestellt, dass sie nach den festgelegten Verfahren dokumentiert und weitergegeben wird (siehe 5.27);

- j) Identifizierung und Behebung von Schwachstellen in der Informationssicherheit, einschließlich der Schwachstellen in Bezug auf Maßnahmen, die den Vorfall verursacht, zu ihm beigetragen oder ihn nicht verhindert haben.

Weitere Informationen

Die Normenreihe ISO/IEC 27035 enthält weitere Anleitungen zur Handhabung von Vorfällen.

5.27 Erkenntnisse aus Informationssicherheitsvorfällen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse sollten zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.

Zweck

Verringerung der Wahrscheinlichkeit oder der Folgen zukünftiger Vorfälle.

Leitfaden

Die Organisation sollte Verfahren zur Quantifizierung und Überwachung von Art, Umfang und Kosten von Informationssicherheitsvorfällen einführen.

Die durch die Bewertung von Informationssicherheitsvorfällen erhaltenen Informationen sollten dazu verwendet werden,

- den Plan für die Handhabung von Vorfällen zu verbessern, einschließlich der Szenarien und Verfahren für Vorfälle (siehe 5.24);
- wiederkehrende oder schwerwiegende Vorfälle und deren Ursachen zu identifizieren, um die Risikobeurteilung der Organisation in Bezug auf die Informationssicherheit zu aktualisieren und die notwendigen zusätzlichen Maßnahmen zur Verringerung der Wahrscheinlichkeit oder der Folgen künftiger ähnlicher Vorfälle zu bestimmen und umzusetzen. Zu den Mechanismen, die dies ermöglichen, gehören die Erfassung, Quantifizierung und Überwachung von Informationen über Art, Umfang und Kosten von Vorfällen;
- die Sensibilisierung und Schulung der Nutzer (siehe 6.3) zu verbessern, indem Beispiele dafür gegeben werden, was passieren kann, wie auf solche Vorfälle zu reagieren ist und wie sie in Zukunft vermieden werden können.

Weitere Informationen

Die Normenreihe ISO/IEC 27035 enthält weitere Anleitungen.

5.28 Sammeln von Beweismaterial

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Die Organisation sollte Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.

Zweck

Sicherstellung einer konsistenten und effektiven Verwaltung von Beweisen im Zusammenhang mit Informationssicherheitsvorfällen für die Zwecke von Maßregelungsmaßnahmen und gerichtlichen Schritten.

Leitfaden

Es sollten interne Verfahren zum Umgang mit Beweismaterial im Zusammenhang mit Informationssicherheitsvorfällen für die Zwecke von Maßregelungsmaßnahmen und gerichtlichen Schritten entwickelt und angewendet werden. Die Anforderungen der verschiedenen Rechtsordnungen sollten beachtet werden, damit die Wahrscheinlichkeit der rechtsordnungsübergreifenden Anerkennung möglichst groß ist.

Allgemein sollten diese Verfahren für die Verwaltung von Beweismaterial Anweisungen zur Identifizierung, Sammlung, Erfassung und Aufbewahrung von entsprechend den verschiedenen Arten von Speichermedien, Geräten und Gerätestatus (d. h. ein- oder ausgeschaltet) bereitstellen. Das Beweismaterial muss in der Regel so erfasst werden, dass es vor den zuständigen nationalen Gerichten oder einem anderen Disziplinarorgan zulässig ist. Es sollte möglich sein, zu zeigen, dass

- die Aufzeichnungen vollständig sind und in keiner Weise manipuliert wurden,
- Kopien von elektronischem Beweismaterial wahrscheinlich mit den Originalen identisch sind,
- alle Informationssysteme, aus denen Beweismaterial entnommen wurde, zum Zeitpunkt der Aufzeichnung des Beweismaterials ordnungsgemäß funktioniert haben.

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

Digitales Beweismaterial kann mehrere Organisationen oder Rechtsordnungen berühren. In derartigen Fällen sollte sichergestellt werden, dass die Organisation befugt ist, die erforderlichen Informationen als digitales Beweismaterial zu sammeln.

Weitere Informationen

Bei Erkennung eines Informationssicherheitsereignisses ist nicht immer 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 Rechtsbeistand oder die Strafverfolgungsbehörden hinzuzuziehen und einen Rat bezüglich des erforderlichen Beweismaterials einzuholen.

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

Die Normenreihe ISO/IEC 27050 befasst sich mit der elektronischen Beweisführung, d.h. mit der Verarbeitung elektronisch gespeicherter Informationen als Beweismaterial.

5.29 Informationssicherheit bei Störungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren	#Aufrechterhaltung	#Schutz #Resilienz

Maßnahme

Die Organisation sollte planen, wie die Informationssicherheit während der Störung auf einem angemessenen Niveau gehalten werden kann.

Zweck

Schutz von Informationen und anderen zugehörigen Werten während einer Störung.

Leitfaden

Die Organisation sollte ihre Anforderungen für die Anpassung der Informationssicherheitsmaßnahmen während einer Störung festlegen. Die Anforderungen an die Informationssicherheit sollten in die Prozesse zum Business Continuity Management einbezogen werden.

Es sollten Pläne zur Aufrechterhaltung oder Wiederherstellung der Informationssicherheit kritischer Geschäftsprozesse nach einer Störung oder einem Ausfall entwickelt, umgesetzt, geprüft, überarbeitet und bewertet werden. Die Sicherheit der Informationen sollte auf der erforderlichen Stufe und innerhalb des erforderlichen Zeitrahmens wiederhergestellt werden.

Die Organisation sollte Folgendes umsetzen und aufrechterhalten:

- Maßnahmen zur Informationssicherheit, unterstützende Systeme und Instrumente im Rahmen von Plänen zur Aufrechterhaltung des Geschäftsbetriebs und der IKT-Kontinuität;
- Prozesse zur Aufrechterhaltung der bestehenden Informationssicherheitsmaßnahmen bei einer Störung;
- Ersatzmaßnahmen für Informationssicherheitsmaßnahmen, die bei einer Störung nicht aufrechterhalten werden können.

Weitere Informationen

Im Zusammenhang mit der Planung der Geschäftskontinuität und der IKT-Kontinuität kann es erforderlich sein, die Anforderungen an die Informationssicherheit je nach Art der Störung im Vergleich zu normalen Betriebsbedingungen anzupassen. Im Rahmen der Analyse der Auswirkungen auf das Geschäft und der Risikobeurteilung, die im Rahmen des Business Continuity Management durchgeführt wird, sollten die Folgen des Verlusts der Vertraulichkeit und der Integrität von Informationen zusätzlich zur Notwendigkeit der Aufrechterhaltung der Verfügbarkeit berücksichtigt und priorisiert werden.

Informationen zum Business Continuity Management können ISO 22301 und ISO 22313 entnommen werden. Weitere Anleitungen zur Analyse der Auswirkungen auf das Geschäft (BIA) sind in ISO/TS 22317 zu finden.

5.30 IKT-Bereitschaft für Business Continuity

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Korrektiv	#Verfügbarkeit	#Reagieren	#Aufrechterhaltung	#Resilienz

Maßnahme

Die IKT-Bereitschaft sollte auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.

Zweck

Sicherstellung der Verfügbarkeit der Informationen in der Organisation und anderer zugehöriger Werte während einer Störung.

Leitfaden

Die IKT-Bereitschaft für Business Continuity ist ein wichtiger Bestandteil des Managements der Geschäftskontinuität und der Informationssicherheit, um sicherzustellen, dass die Ziele der Organisation während einer Störung weiterhin erreicht werden können.

Die Anforderungen an die IKT-Kontinuität sind das Ergebnis der Analyse der geschäftlichen Auswirkungen (BIA). Der BIA-Prozess sollte Auswirkungsarten und -kriterien verwenden, um die Auswirkungen zu beurteilen, die sich im Laufe der Zeit aus der Störung von Geschäftsaktivitäten ergeben, die Produkte und Dienstleistungen liefern. Anhand des Ausmaßes und der Dauer der daraus resultierenden Auswirkungen sollten vorrangige Aktivitäten ermittelt werden, denen eine Wiederherstellungsdauer (RTO) zugewiesen werden sollte. Die BIA sollte dann festlegen, welche Ressourcen zur Unterstützung der priorisierten Betriebstätigkeiten benötigt werden. Für diese Ressourcen sollte auch eine RTO angegeben werden. Eine Teilmenge dieser Ressourcen sollte IKT-Dienste umfassen.

Die BIA, die IKT-Dienste einbezieht, kann erweitert werden, um die Leistungs- und Kapazitätsanforderungen von IKT-Systemen und Wiederherstellungspunkte (RPO) von Informationen zu definieren, die zur Unterstützung von Aktivitäten während einer Störung erforderlich sind.

Auf der Grundlage der Ergebnisse der BIA und der Risikobeurteilung für IKT-Dienste sollte die Organisation IKT-Kontinuitätsstrategien ermitteln und auswählen, die Optionen für die Zeit vor, während und nach einer Störung berücksichtigen. Die Strategien zur Aufrechterhaltung des Geschäftsbetriebs können eine oder mehrere Lösungen umfassen. Auf der Grundlage der Strategien sollten Pläne entwickelt, umgesetzt und geprüft werden, um die erforderliche Verfügbarkeit von IKT-Diensten nach einer Störung oder einem Ausfall kritischer Prozesse innerhalb des erforderlichen Zeitrahmens zu erfüllen.

Die Organisation sollte folgende Punkte sicherstellen:

- a) Vorhandensein einer angemessenen Organisationsstruktur zur Vorbereitung, Eindämmung und Reaktion in Bezug auf eine Störung unterstützt durch Personal mit der erforderlichen Verantwortung, Befugnis und Kompetenz;
- b) IKT-Kontinuitätspläne, einschließlich Reaktions- und Wiederherstellungsverfahren, die detailliert beschreiben, wie die Organisation mit einer Störung der IKT-Dienste umzugehen gedenkt, sind;

- 1) regelmäßig durch Übungen und Prüfungen bewertet worden;
 - 2) vom Management genehmigt;
- c) Die IKT-Kontinuitätspläne enthalten die folgenden Informationen zur IKT-Kontinuität:
- 1) Leistungs- und Kapazitätsspezifikationen zur Erfüllung der in der BIA festgelegten Anforderungen und Ziele der Aufrechterhaltung der Betriebsfähigkeit;
 - 2) RTO der einzelnen priorisierten IKT-Dienste und die Verfahren zur Wiederherstellung dieser Komponenten;
 - 3) RPO der priorisierten IKT-Ressourcen, die als Informationen definiert sind, und die Verfahren zur Wiederherstellung der Informationen.

Weitere Informationen

Die Verwaltung der IKT-Kontinuität ist ein wesentlicher Bestandteil der Anforderungen an die Aufrechterhaltung der Betriebsfähigkeit in Bezug auf die Verfügbarkeit, um in der Lage zu sein:

- a) auf Störungen von IKT-Diensten unabhängig von deren Ursache zu reagieren und diese zu beheben;
- b) die Kontinuität der priorisierten Betriebstätigkeit durch die erforderlichen IKT-Dienste sicherzustellen;
- c) zu reagieren, bevor es zu einer Störung der IKT-Dienste kommt, und wenn mindestens ein Vorfall festgestellt wird, der zu einer Störung der IKT-Dienste führen kann.

Weitere Anleitungen zur IKT-Bereitschaft für die Aufrechterhaltung der Business Continuity sind in ISO/IEC 27031 zu finden.

Weitere Anleitungen zum Business Continuity Management können ISO 22301 und ISO 22313 entnommen werden.

Weitere Anleitungen zur BIA sind in ISO/TS 22317 zu finden.

5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Recht_und_Compliance	#Governance_und_Ökosystem #Schutz

Maßnahme

Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen sollten ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.

Zweck

Sicherstellung der Einhaltung rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen in Bezug auf die Informationssicherheit.

Leitfaden

Allgemeines

Externe Anforderungen, einschließlich rechtlicher, gesetzlicher, regulatorischer oder vertraglicher Anforderungen, sollten berücksichtigt werden:

- a) bei Entwicklung von Richtlinien und Verfahren für die Informationssicherheit;
- b) bei Gestaltung, Implementierung oder Änderung von Informationssicherheitsmaßnahmen;
- c) bei Klassifizierung von Informationen und anderen zugehörigen Werten als Teil des Prozesses zur Festlegung von Anforderungen an die Informationssicherheit für den internen Bedarf oder für Lieferantenvereinbarungen;
- d) bei Durchführung von Risikobeurteilungen der Informationssicherheit und Festlegung von Maßnahmen zur Behandlung von Risiken der Informationssicherheit;
- e) bei Festlegung von Prozessen sowie der damit verbundenen Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit;
- f) bei Bestimmung der vertraglichen Anforderungen der Lieferanten, die für die Organisation und den Umfang der Lieferung von Produkten und Dienstleistungen relevant sind.

Gesetzgebung und Vorschriften

Die Organisation sollte:

- a) alle für die Informationssicherheit der Organisation relevanten Gesetze und Vorschriften ermitteln, um sich über die Anforderungen für ihre Art von Geschäft im Klaren zu sein;
- b) die Einhaltung der Vorschriften in allen relevanten Ländern berücksichtigen, wenn die Organisation:
 - Geschäfte in anderen Ländern tätigt;
 - Produkte und Dienstleistungen aus anderen Ländern nutzt, in denen Gesetze und Vorschriften die Organisation beeinflussen können;
 - Informationen über Ländergrenzen hinweg überträgt, in denen Gesetze und Vorschriften das Unternehmen beeinflussen können;
- c) die ermittelten Rechtsvorschriften und Regelungen regelmäßig überprüfen, um über die Änderungen auf dem Laufenden zu bleiben und neue Rechtsvorschriften zu ermitteln;
- d) die spezifischen Prozesse und individuellen Verantwortlichkeiten zur Erfüllung dieser Anforderungen definieren und dokumentieren.

Kryptographie

Die Kryptographie ist ein Bereich, für den häufig besondere rechtliche Anforderungen gelten. Die Einhaltung der einschlägigen Vereinbarungen, Gesetze und Vorschriften in Bezug auf die folgenden Punkte sollte 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 der Kryptographie;
- d) verpflichtende oder freiwillige Verfahren für den Zugriff der Behörden der Länder auf verschlüsselte Informationen;
- e) die Gültigkeit von digitalen Signaturen, Siegeln und Zertifikaten.

Es wird empfohlen, sich rechtlich beraten zu lassen, wenn es darum geht, die Einhaltung einschlägiger Gesetze und Vorschriften sicherzustellen, insbesondere wenn verschlüsselte Informationen oder Kryptographietools über Ländergrenzen hinweg transportiert werden.

Verträge

Zu den vertraglichen Anforderungen in Bezug auf die Informationssicherheit sollten u. a. gehören:

- a) die in den Verträgen mit Kunden genannten;
- b) die in den Verträgen mit Lieferanten genannten (siehe 5.20);
- c) die in Versicherungsverträgen genannten.

Weitere Informationen

Keine weiteren Informationen.

5.32 Geistige Eigentumsrechte

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Recht_und_Compliance	#Governance_und_Ökosystem

Maßnahme

Die Organisation sollte geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.

Zweck

Sicherstellung der Einhaltung rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und die Verwendung von urheberrechtlich geschützten Produkten.

Leitfaden

Die folgenden Leitfäden sollten zum Schutz von jedwedem Material berücksichtigt werden, das als geistiges Eigentum betrachtet werden kann:

- a) Festlegung und Bekanntgabe einer themenspezifischen Richtlinie zum Schutz der Rechte an geistigem Eigentum;
- b) Veröffentlichung von Verfahren zur Einhaltung von Rechten an geistigem Eigentum, die die vorschriftsmäßige Nutzung von Software und Informationsprodukten festlegen;
- c) Bezug von Software nur über bekannte und seriöse Quellen, um sicherzustellen, dass das Urheberrecht nicht verletzt wird;
- d) Führen entsprechender Werteregister und Feststellung aller Werte mit Schutzanforderungen bezüglich der geistigen Eigentumsrechte;
- e) Aufbewahrung von Nachweisen und Beweismaterial für die Inhaberschaft von Lizenzen, Handbüchern usw.;
- f) Sicherstellung, dass die im Rahmen der Lizenz zulässige Höchstzahl von Benutzern oder Ressourcen [z. B. Prozessoren (CPUs)] nicht überschritten wird;
- g) Durchführung von Überprüfungen, um sicherzustellen, dass nur genehmigte Software und lizenzierte Produkte installiert sind;
- h) Bereitstellung von Verfahren zur Einhaltung der entsprechenden Lizenzbedingungen;
- i) Bereitstellung von Verfahren zur Veräußerung, Entsorgung oder Weitergabe von Software an andere;
- j) Einhaltung der Bedingungen und Konditionen in Bezug auf Software und Informationen, die aus öffentlichen Netzen und externen Quellen stammen;
- k) keine Vervielfältigung, Formatkonvertierung oder Verwendung von Auszügen kommerzieller Aufzeichnungen (Video, Audio), die nach dem Urheberrecht oder den geltenden Lizenzen untersagt ist;
- l) keine Anfertigung von vollständigen oder auszugsweisen Kopien von Normen (z. B. ISO/IEC Internationale Normen), Büchern, Artikeln, Berichten oder anderen Dokumenten, die nach dem Urheberrecht oder den geltenden Lizenzen untersagt ist.

Weitere Informationen

Die geistigen Eigentumsrechte beinhalten das Urheberrecht an Software und Dokumenten, Geschmacksmustern, Markenzeichen, Patenten 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. Siehe die Normenreihe ISO/IEC 19770 für Einzelheiten zum Management von IT-Werten.

Die Daten können aus externen Quellen bezogen werden. Im Allgemeinen werden solche Daten im Rahmen einer Vereinbarung über die gemeinsame Nutzung von Daten oder eines ähnlichen Rechtsinstruments erhoben. Aus solchen Vereinbarungen über die gemeinsame Nutzung von Daten sollte klar hervorgehen, welche Verarbeitung der erworbenen Daten zulässig ist. Es ist auch ratsam, dass die Herkunft der Daten klar angegeben wird. Siehe ISO/IEC 23751 für Einzelheiten zu Vereinbarungen über die gemeinsame Nutzung von Daten.

Rechtliche, gesetzliche, regulatorische 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.

Abgesehen davon, dass die Organisation ihre Verpflichtungen gegenüber den Rechten am geistigen Eigentum Dritter einhalten muss, sollten auch die Risiken von Personal und Dritten, die die Rechte am geistigen Eigentum der Organisation verletzen, berücksichtigt werden.

5.33 Schutz von Aufzeichnungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Recht_und_Compliance #Asset_Management #Informationsschutz	#Verteidigung

Maßnahme

Aufzeichnungen sollten vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.

Zweck

Sicherstellung der Einhaltung rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen sowie von Erwartungen der Gemeinschaft oder der Gesellschaft in Bezug auf den Schutz und die Verfügbarkeit von Unterlagen.

Leitfaden

Die Organisation sollte die folgenden Schritte unternehmen, um die Authentizität, Zuverlässigkeit, Integrität und Verwendbarkeit von Aufzeichnungen zu schützen, da sich der geschäftliche Kontext und die Anforderungen an ihre Verwaltung im Laufe der Zeit ändern:

- Herausgabe von Richtlinien für die Aufbewahrung, den Umgang mit der Aufbewahrungskette und die Entsorgung von Unterlagen, die auch die Verhinderung von Manipulationen an Unterlagen umfassen. Diese Richtlinien sollten mit den themenspezifischen Richtlinien der Organisation zur Verwaltung von Unterlagen und anderen Anforderungen an Unterlagen abgestimmt werden;
- Erstellung eines Zeitplans für die Aufbewahrung von Unterlagen und den Zeitraum, in dem sie aufbewahrt werden müssen.

Das System zur Speicherung- und Handhabung sollte sofern zutreffend die Kennzeichnung von Aufzeichnungen und ihrer Aufbewahrungsfrist unter Berücksichtigung nationaler oder regionaler Gesetze oder Verordnungen sowie die Erwartungen der Gemeinschaft oder der Gesellschaft sicherstellen. Dieses System sollte die entsprechende Vernichtung von Aufzeichnungen nach Ablauf dieser Frist ermöglichen, falls die Organisation sie nicht mehr benötigt.

Bei der Entscheidung über den Schutz bestimmter Aufzeichnungen der Organisation sollten die entsprechenden Klassifizierungen der Informationssicherheit auf Grundlage des Klassifizierungsschemas der Organisation berücksichtigt werden. Die Aufzeichnungen sollten nach Aufzeichnungsarten kategorisiert werden (z. B. Geschäftsbücher, Aufzeichnungen über Geschäftsvorgänge, Personalaufzeichnungen, rechtliche Aufzeichnungen), jeweils mit Angaben zu den Aufbewahrungsfristen und der Art der zulässigen Speichermedien, die physisch oder elektronisch sein können.

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

Bei der Wahl elektronischer Speichermedien sollten Verfahren festgelegt werden, durch die der Zugriff auf die Aufzeichnungen (hinsichtlich der Lesbarkeit der Speichermedien als auch des Formats) über den gesamten Aufbewahrungszeitraum sichergestellt ist, um vor Datenverlust aufgrund zukünftiger technischer Veränderungen geschützt zu sein. Alle kryptographischen Schlüssel und Programme, die für verschlüsselte Archive oder digitale Signaturen benötigt werden, sollten ebenfalls aufbewahrt werden, um eine Entschlüsselung der Aufzeichnungen für den Zeitraum ihrer Aufbewahrung (siehe 8.24) zu ermöglichen.

Die Verfahren zu Speicherung und Umgang sollten entsprechend den Empfehlungen der Hersteller von Speichermedien durchgeführt werden. Es sollte die Möglichkeit der Verschlechterung der für die Speicherung der Aufzeichnungen verwendeten Datenträger in Betracht gezogen werden.

Weitere Informationen

Aufzeichnungen dokumentieren einzelne Ereignisse oder Transaktionen oder können Aggregationen bilden, die zur Dokumentation von Arbeitsabläufen, Aktivitäten oder Funktionen konzipiert wurden. Sie sind sowohl ein Beweis für geschäftliche Aktivitäten als auch ein Informationswert. Jede Information, unabhängig von ihrer Struktur oder Form, kann als Datensatz verwaltet werden. Dazu gehören Informationen in Form eines Dokuments, einer Datensammlung oder anderer Arten von digitalen oder analogen Informationen, die im Rahmen der Geschäftstätigkeit erstellt, erfasst und verwaltet werden.

Bei der Verwaltung von Aufzeichnungen handelt es sich bei Metadaten um Daten, die den Kontext, den Inhalt und die Struktur von Aufzeichnungen sowie deren Verwaltung im Laufe der Zeit beschreiben. Metadaten sind ein wesentlicher Bestandteil eines jeden Datensatzes.

Es kann notwendig sein, einige Aufzeichnungen sicher aufzubewahren, um rechtliche, gesetzliche, regulatorische oder vertragliche Anforderungen zu erfüllen und um wesentliche Geschäftsaktivitäten zu unterstützen. Der Aufbewahrungszeitraum und der Umfang der aufzubewahrenden Informationen können durch nationale Gesetze oder Bestimmungen vorgegeben sein. Weitere Informationen zum Umgang mit den Aufzeichnungen können ISO 15489 entnommen werden.

5.34 Datenschutz und Schutz personenbezogener Daten (pbD)

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Informationsschutz #Recht_und_Compliance	#Schutz

Maßnahme

Die Organisation sollte die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.

Zweck

Sicherstellung der Einhaltung rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen in Bezug auf die Informationssicherheitsaspekte des Schutzes personenbezogener Daten.

Leitfaden

Die Organisation sollte eine themenspezifische Richtlinie zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten einführen und allen relevanten interessierten Parteien mitteilen.

Die Organisation sollte Verfahren zur Wahrung der Privatsphäre und zum Schutz personenbezogener Daten entwickeln und umsetzen. Diese Verfahren sollten allen relevanten interessierten Parteien bekanntgemacht werden, die in die Verarbeitung personenbezogener Informationen einbezogen sind.

Die Einhaltung dieser Verfahren und aller einschlägigen Gesetze und Vorschriften zur Wahrung der Privatsphäre und zum Schutz personenbezogener Daten erfordert angemessene Rollen, Verantwortlichkeiten und Maßnahmen. Am besten kann dies meist durch Benennung einer dafür zuständigen Person wie eines Datenschutzbeauftragten erreicht werden, der dem Personal, den Dienstleistern und anderen interessierten Parteien eine Richtschnur hinsichtlich ihrer jeweiligen Verantwortungsbereiche sowie der jeweils einzuhaltenden Verfahren vorgibt.

Die Verantwortung für den Umgang mit personenbezogenen Daten sollte unter Berücksichtigung der einschlägigen Gesetze und Vorschriften geregelt werden.

Es sollten geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten umgesetzt werden.

Weitere Informationen

Einige Länder haben Gesetze zur Steuerung der Erhebung, Verarbeitung, Übermittlung und Löschung personenbezogener Daten erlassen. In Abhängigkeit von den jeweiligen nationalen Gesetzen können derartige Maßnahmen die Auferlegung bestimmter Pflichten bei der Erhebung, Verarbeitung und Weitergabe personenbezogener Daten sowie eine Einschränkung der Befugnis zur Übermittlung von pbD in andere Länder beinhalten.

ISO/IEC 29100 bietet einen groben Rahmen für den Schutz personenbezogener Informationen im Rahmen von IKT-Systemen. Weitere Informationen über Datenschutz-Informationsmanagementsysteme sind in ISO/IEC 27701 zu finden. Spezifische Angaben zum Datenschutzmanagement für öffentliche Clouds, die als Auftragsdatenverarbeiter fungieren, können ISO/IEC 27018 entnommen werden.

ISO/IEC 29134 enthält Leitlinien für die Datenschutz-Folgenabschätzung (DSFA) und gibt ein Beispiel für die Struktur und den Inhalt eines DSFA-Berichts. Im Vergleich zu ISO/IEC 27005 ist diese Norm auf die Verarbeitung personenbezogener Daten ausgerichtet und für Organisationen relevant, die personenbezogene Daten verarbeiten. Dies kann dazu beitragen, Risiken für die Privatsphäre und mögliche Abhilfemaßnahmen zu ermitteln, um diese Risiken auf ein annehmbares Niveau zu reduzieren.

5.35 Unabhängige Überprüfung der Informationssicherheit

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Identifizieren	#Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit	#Governance_und_Ökosystem
#Korrektiv	#Integrität #Verfügbarkeit	#Schützen		

Maßnahme

Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, sollten auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.

Zweck

Sicherstellung der dauerhaften Eignung, Angemessenheit und Wirksamkeit des Ansatzes der Organisation in Bezug auf die Handhabung von Informationssicherheit.

Leitfaden

Die Organisation sollte über Verfahren zur Durchführung unabhängiger Überprüfungen verfügen.

Das Management sollte regelmäßige unabhängige Überprüfungen planen und veranlassen. Diese Überprüfungen sollten eine Beurteilung von Verbesserungsmöglichkeiten und ggf. vorhandenem Änderungsbedarf bezüglich des Informationssicherheitsansatzes einschließlich der Informationssicherheitspolitik, themenspezifischer Richtlinien und anderer Maßnahmen beinhalten.

Diese Überprüfungen sollten von Personen durchgeführt werden, die unabhängig vom untersuchten Bereich sind (z. B. ein interner Auditor, ein unabhängiger Manager oder eine externe Organisation, die sich auf derartige Prüfungen spezialisiert hat). Die diese Prüfungen durchführenden Personen sollten über entsprechende Kompetenzen verfügen. Die Person, die die Überprüfungen durchführt, sollte nicht in der Hierarchie stehen, um sicherzustellen, dass sie die nötige Unabhängigkeit hat, um eine Beurteilung vornehmen zu können.

Die Ergebnisse der unabhängigen Prüfungen sollten an das Management, das die Prüfungen veranlasst hat, und gegebenenfalls der obersten Leitung berichtet werden. Diese Aufzeichnungen sollten aufbewahrt werden.

Sollten bei den unabhängigen Prüfungen 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 der Informationssicherheitspolitik und den themenspezifischen Richtlinien (siehe 5.1) festgelegten Richtung entsprechen] sollte das Management Korrekturmaßnahmen veranlassen.

Zusätzlich zu den regelmäßigen unabhängigen Überprüfungen sollte die Organisation erwägen, unabhängige Überprüfungen durchzuführen, wenn:

- a) Gesetze und Vorschriften, die das Unternehmen betreffen, sich ändern;
- b) signifikante Vorfälle auftreten;
- c) die Organisation ein neues Geschäft eröffnet oder ein bestehendes Geschäft ändert;
- d) die Organisation ein neues Produkt oder eine neue Dienstleistung einsetzt oder den Einsatz eines bestehenden Produkts oder einer bestehenden Dienstleistung ändert;
- e) die Organisation Informationssicherheitsmaßnahmen und -verfahren erheblich ändert.

Weitere Informationen

ISO/IEC 27007 und ISO/IEC TS 27008 bieten eine Anleitung zur Durchführung unabhängiger Überprüfungen.

5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Recht_und_Compliance #Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit	#Governance_und_Ökosystem

Maßnahme

Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen sollte regelmäßig überprüft werden.

Zweck

Sicherstellung, dass die Informationssicherheit in Übereinstimmung mit der Informationssicherheitspolitik der Organisation, themenspezifischen Richtlinien, Regeln und Normen umgesetzt und betrieben wird.

Leitfaden

Leitende Angestellte, Dienstleistungs-, Produkt- oder Informationseigentümer sollten festlegen, wie die Einhaltung von in der Informationssicherheitspolitik, in themenspezifischen Richtlinien, Regeln, Normen und anderen geltenden Vorschriften festgelegten Informationssicherheitsanforderungen überprüft wird. Automatische Werkzeuge zur Bewertung und Berichterstattung sollten bei einer effizienten, regelmäßigen Prüfung berücksichtigt werden.

Falls bei der Prüfung ein Compliance-Verstoß festgestellt wird, sollten die Manager die folgenden Maßnahmen ergreifen:

- a) Feststellung der Ursachen des Compliance-Verstoßes;
- b) Beurteilung, ob Korrekturmaßnahmen zur Herstellung der Compliance 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, Dienstleistungs-, Produkt- oder Informationseigentümern 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 5.35), wenn in ihrem Verantwortungsbereich eine unabhängige Prüfung stattfindet.

Korrekturmaßnahmen sollten je nach Risiko zeitnah durchgeführt werden. Wenn sie nicht bis zur nächsten geplanten Überprüfung abgeschlossen sind, sollten die Fortschritte zumindest bei dieser Überprüfung angesprochen werden.

Weitere Informationen

Die betriebliche Überwachung der Systemnutzung wird in 8.15, 8.16, 8.17 behandelt.

5.37 Dokumentierte Betriebsabläufe

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Asset_Management	#Governance_und_Ökosystem
#Korrektiv	#Integrität #Verfügbarkeit	#Wiederherstellen	#Physische_Sicherheit #System- und Netzwerksicherheit #Anwendungssicherheit #Sichere_Konfiguration #Identitäts- und Zugangsverwaltung #Bedrohungs- und Schwachstellenmanagement #Aufrechterhaltung #Handhabung_von_Informationssicherheitsereignissen	#Schutz #Verteidigung

Maßnahme

Die Betriebsverfahren für Informationsverarbeitungsanlagen sollten dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.

Zweck

Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.

Leitfaden

Es sollten dokumentierte Verfahren für die betrieblichen Aktivitäten der Organisation im Zusammenhang mit der Informationssicherheit ausgearbeitet werden, z. B.:

- a) wenn die Tätigkeit von vielen Personen auf die gleiche Weise ausgeführt werden muss;
- b) wenn die Tätigkeit selten ausgeübt wird und das Verfahren bei der nächsten Ausführung wahrscheinlich vergessen wurde;
- c) wenn die Tätigkeit neu ist und ein Risiko darstellt, wenn sie nicht korrekt ausgeführt wird;
- d) vor der Übergabe der Tätigkeit an neues Personal.

Die Betriebsverfahren sollten Folgendes festlegen:

- a) die verantwortlichen Personen;
- b) die sichere Installation und Konfiguration der Systeme;
- c) Verarbeitung von und Umgang mit Informationen (automatisiert und manuell);
- d) Sicherung (siehe 8.13) und Ausfallsicherheit;
- e) Anforderungen an die Zeitplanung, einschließlich der Abhängigkeiten von anderen Systemen;
- f) Anweisungen zur Behandlung von Fehlern oder anderen außergewöhnlichen Bedingungen [z. B. Einschränkungen bei der Verwendung von Hilfsprogrammen (siehe 8.18)], die während der Auftragsausführung auftreten können;
- g) Ansprechpartner für Support und Eskalation einschließlich der Ansprechpartner für den Support bei unerwarteten betrieblichen oder technischen Schwierigkeiten;
- h) Anweisungen zur Handhabung von Speichermedien (siehe 7.10 und 7.14);
- i) Verfahren für System-Neustart und Wiederherstellung zur Nutzung bei einem Systemausfall;
- j) die Verwaltung von Prüfpfad- und Systemprotokolldaten (siehe 8.15 und 8.17) und Videoüberwachungssystemen (siehe 7.4);
- k) Überwachungsverfahren wie Kapazität, Leistung und Sicherheit (siehe 8.6 und 8.16);
- l) Wartungsvorschriften.

Die dokumentierten Betriebsverfahren sollten überprüft und bei Bedarf aktualisiert werden. Änderungen an dokumentierten Betriebsverfahren sollten genehmigt werden. Informationssysteme sollten, sofern dies technisch durchführbar ist, zentral mittels derselben Verfahren, Werkzeuge und Dienstprogramme verwaltet werden.

Weitere Informationen

Keine weiteren Informationen.

6 Personenbezogene Maßnahmen

6.1 Sicherheitsüberprüfung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Humanressourcen	#Governance_und_Ökosystem

Maßnahme

Alle Personen, die in die Belegschaft aufgenommen werden, sollten vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.

Zweck

Sicherstellung, dass alle Mitarbeiter für die Aufgaben, für die sie in Frage kommen, geeignet sind und während ihrer Beschäftigung geeignet bleiben.

Leitfaden

Ein Screening sollte für das gesamte Personal, einschließlich Vollzeit-, Teilzeit- und Zeitarbeitskräfte, durchgeführt werden. Wenn diese Personen über Dienstleistungsanbieter unter Vertrag genommen werden, sollten die Anforderungen an die Überprüfung in die vertraglichen Vereinbarungen zwischen der Organisation und den Anbietern aufgenommen werden.

Informationen über alle Bewerber, die für Positionen in der Organisation infrage kommen, sollten unter Berücksichtigung entsprechender Gesetze in der jeweiligen Rechtsordnung gesammelt und verarbeitet werden. In einigen Rechtsordnungen kann die Organisation gesetzlich verpflichtet sein, die Bewerber vorab über die Überprüfungsmaßnahmen zu informieren.

Überprüfungen sollten alle einschlägigen Rechtsvorschriften zum Schutz der Privatsphäre, zum Schutz personenbezogener Daten und zur Beschäftigung berücksichtigen und, sofern erlaubt, Folgendes einschließen:

- a) Vorhandensein zufriedenstellender Referenzen, z. B. dienstliche und persönliche Zeugnisse);
- b) ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers;
- c) Bestätigung angegebener akademischer und beruflicher Qualifikationen;
- d) unabhängige Identitätsüberprüfung (z. B. Reisepass oder ein anderes akzeptables, von den zuständigen Behörden ausgestelltes Dokument);
- e) detailliertere Nachweise, wie Bonitätsprüfung oder Überprüfung des Strafregisters, wenn der Bewerber eine kritische Rolle einnimmt.

Wenn eine Person für eine bestimmte Rolle der Informationssicherheit angestellt wird, sollte die Organisation sicherstellen, dass der Bewerber:

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

Falls eine ersteingestellte oder beförderte Person Zugang zu informationsverarbeitenden Einrichtungen hat, die insbesondere den Umgang mit vertraulichen Informationen (z. B. Finanzdaten, persönliche Daten oder Informationen aus dem Gesundheitswesen) beinhalten, sollte die Organisation weitere, eingehendere Überprüfungen in Betracht ziehen.

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

In Situationen, in denen die Überprüfung nicht rechtzeitig abgeschlossen werden kann, sollten abmildernde Maßnahmen ergriffen werden, bis die Überprüfung abgeschlossen ist, z. B.:

- a) verzögerte Einarbeitung;
- b) verzögerter Einsatz von Unternehmensvermögen;
- c) Einarbeitung mit eingeschränktem Zugang;
- d) Beendigung der Beschäftigung.

Die Überprüfungen sollten in regelmäßigen Abständen wiederholt werden, um die kontinuierliche Eignung des Personals zu bestätigen, je nachdem, wie kritisch die Rolle der betreffenden Person ist.

Weitere Informationen

Keine weiteren Informationen.

6.2 Beschäftigungs- und Vertragsbedingungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Humanressourcen	#Governance_und_Ökosystem

Maßnahme

In den arbeitsvertraglichen Vereinbarungen sollten die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.

Zweck

Es ist sichergestellt, dass die Mitarbeiter ihre Verantwortung für die Informationssicherheit in den für sie vorgesehenen Rollen verstehen.

Leitfaden

Die Arbeitsvertragsklauseln für das Personal sollten die Informationssicherheitspolitik der Organisation und die einschlägigen themenspezifischen Richtlinien berücksichtigen. Zusätzlich können die folgenden Punkte geklärt und festgehalten werden:

- a) Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die Mitarbeiter, die Zugang zu vertraulichen Informationen erhalten, unterzeichnen sollten, bevor sie Zugang zu Informationen und anderen damit verbundenen Werten erhalten (siehe 6.6);
- b) gesetzliche Verantwortlichkeiten und Rechte [z. B. in Bezug auf Urheberrechtsgesetze oder Datenschutzgesetze (siehe 5.32 und 5.34)];
- c) Verantwortungen für die Klassifizierung von Informationen und die Verwaltung der Informationen der Organisation und anderer zugehöriger Werte, der Informationsverarbeitungseinrichtungen und der Informationsdienste, die vom Personal verarbeitet werden (siehe 5.9 bis 5.13);
- d) Verantwortlichkeiten für den Umgang mit Informationen, die von interessierten Parteien stammen;
- e) Maßnahmen, die ergriffen werden müssen, wenn das Personal die Sicherheitsanforderungen der Organisation missachtet (siehe 6.4).

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

Die Organisation sollte sicherstellen, dass das Personal den Geschäftsbedingungen für die Informationssicherheit zustimmt. Diese Geschäftsbedingungen sollten Art und Umfang des Zugangs zu organisationseigenen Werten im Zusammenhang mit Informationssystemen und -diensten berücksichtigen. Die Geschäftsbedingungen zur Informationssicherheit sollten überprüft werden, wenn sich Gesetze, Vorschriften, die Informationssicherheitspolitik oder themenspezifische Richtlinien ändern.

Gegebenenfalls sollten Verantwortlichkeiten, die in den Beschäftigungsbedingungen angegeben sind, über die Beschäftigungsdauer hinaus für einen bestimmten Zeitraum gelten (siehe 6.5).

Weitere Informationen

Ein Verhaltenskodex kann verwendet werden, um die Verantwortlichkeiten des Personals für die Informationssicherheit in Bezug auf Geheimhaltung, Datenschutz, ethische Grundsätze, angemessene Nutzung der Informationen der Organisation und anderer zugehöriger Werte sowie die von der Organisation erwarteten seriösen Praktiken festzulegen.

Von einer externen Partei, mit der das Personal des Lieferanten assoziiert ist, kann verlangt werden, vertragliche Vereinbarungen im Namen der unter Vertrag genommenen Person einzugehen.

Handelt es sich bei der Organisation nicht um eine juristische Person und hat sie keine Beschäftigten, können die vertraglichen Vereinbarungen und Bedingungen als gleichwertig betrachtet werden, wie in dieser Maßnahme beschrieben.

6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Humanressourcen	#Governance_und_Ökosystem

Maßnahme

Das Personal der Organisation und relevante interessierte Parteien sollten ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.

Zweck

Es ist sichergestellt, dass das Personal und relevante interessierte Parteien sich ihrer Verantwortlichkeiten bezüglich der Informationssicherheit bewusst sind und diesen nachkommen.

Leitfaden

Allgemeines

Ein Sensibilisierungs-, Ausbildungs- und Schulungsprogramm für Informationssicherheit sollte in Einklang mit der Informationssicherheitspolitik der Organisation, den themenspezifischen Richtlinien und den einschlägigen Verfahren zur Informationssicherheit unter Berücksichtigung der zu schützenden Information der Organisation und der schon bestehenden Informationssicherheitsmaßnahmen zum Schutz der Information festgelegt werden.

Die Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit sollte regelmäßig stattfinden. Die erste Sensibilisierung, Ausbildung und Schulung kann für neue Mitarbeiter und für Mitarbeiter gelten, die in neue Positionen oder Rollen mit wesentlich anderen Anforderungen an die Informationssicherheit wechseln.

Das Verständnis des Personals sollte am Ende einer Sensibilisierungs-, Ausbildungs- oder Schulungsmaßnahme beurteilt werden, um den Wissenstransfer und die Wirksamkeit des Sensibilisierungs-, Ausbildungs- und Schulungsprogramms zu prüfen.

Bewusstsein

Ein Sensibilisierungsprogramm für Informationssicherheit sollte darauf abzielen, dass sich das Personal seiner Verantwortung für Informationssicherheit bewusst wird und auf welche Weise diesen Verantwortungen entsprochen wird.

Das Sensibilisierungsprogramm sollte unter Berücksichtigung der Rollen des Personals in der Organisation, einschließlich des internen und externen Personals (z. B. externe Berater, Lieferantenpersonal), geplant werden. Maßnahmen des Sensibilisierungsprogramms sollten vorher zeitlich und vorzugsweise regelmäßig eingeplant werden, damit diese Maßnahmen wiederholt werden und auch neues Personal erfasst wird. Es sollte auch auf den Erkenntnissen aus Vorfällen im Bereich der Informationssicherheit aufbauen.

Das Sensibilisierungsprogramm sollte eine Reihe von Sensibilisierungsmaßnahmen über geeignete physische oder virtuelle Kanäle umfassen, z. B. Kampagnen, Broschüren, Poster, Newsletter, Websites, Informationsveranstaltungen, Briefings, E-Learning-Module und E-Mails.

Das Bewusstsein für die Informationssicherheit sollte auch generelle Aspekte enthalten wie:

- a) Verpflichtung der Leitung zu Informationssicherheit in der gesamten Organisation;
- b) Vertrautheit mit den geltenden Vorschriften und Verpflichtungen im Bereich der Informationssicherheit und deren Einhaltung unter Berücksichtigung der Informationssicherheitspolitik und themenspezifischen Richtlinien, Normen, Gesetze, Statuten, Vorschriften, Verträge und Vereinbarungen;
- c) persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortlichkeiten zur Sicherung oder zum Schutz von Informationen, die der Organisation und interessierten Parteien gehören;
- d) grundsätzliche Verfahren zur Informationssicherheit [z. B. Meldung von Informationssicherheitsereignissen (6.8)] und grundlegende Sicherheitsmaßnahmen [z. B. Kennwortsicherheit (5.17)];
- e) Anlaufstellen und Ressourcen für zusätzliche Informationen und Empfehlungen zu Fragen der Informationssicherheit, einschließlich weiterer Sensibilisierungsunterlagen zur Informationssicherheit.

Aus- und Weiterbildung

Die Organisation sollte einen geeigneten Schulungsplan für technische Teams, deren Aufgaben besondere Fähigkeiten und Fachkenntnisse erfordern, ermitteln, ausarbeiten und umsetzen. Technische Teams sollten über die Fähigkeiten verfügen, das erforderliche Sicherheitsniveau für Geräte, Systeme, Anwendungen und Dienste zu konfigurieren und aufrechtzuerhalten. Wenn es an Fähigkeiten mangelt, sollte die Organisation Maßnahmen ergreifen und diese erwerben.

Für das Aus- und Weiterbildungsprogramm sollten verschiedene Formen in Betracht gezogen werden [z. B. Lehrveranstaltungen oder Selbststudium, Betreuung durch Fachpersonal oder Berater (Ausbildung am Arbeitsplatz), Rotation des Personals für verschiedene Tätigkeiten, Einstellung bereits ausgebildeter Mitarbeiter und Einstellung von Beratern]. Dabei können verschiedene Formen der Vermittlung zum Einsatz kommen, darunter Klassenunterricht, Fernunterricht, internetbasiert, Selbststudium und andere. Das technische Personal sollte sein Wissen auf dem neuesten Stand halten, indem es Newsletter und Zeitschriften abonniert oder an Konferenzen und Veranstaltungen teilnimmt, die der technischen und beruflichen Weiterbildung dienen.

Weitere Informationen

Bei der Ausarbeitung eines Sensibilisierungsprogramms ist wichtig, nicht nur das „Was“ und „Wie“, sondern auch, wenn möglich, das „Warum“ anzusprechen. Es ist wichtig, dass das Personal das Ziel der Informationssicherheit und die möglichen positiven und negativen Auswirkungen seines Verhaltens auf die Organisation versteht.

Sensibilisierung, Ausbildung und Schulung im Bereich der Informationssicherheit können Teil anderer Aktivitäten sein oder in Zusammenarbeit mit diesen durchgeführt werden, z. B. allgemeine Schulungen in den Bereichen Informationsmanagement, IKT, Schutz, Datenschutz oder Sicherheit.

6.4 Maßregelungsprozess

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Sicherheit_der_Humanressourcen	#Governance_und_Ökosystem
#Korrektiv	#Integrität #Verfügbarkeit	#Reagieren		

Maßnahme

Ein Maßregelungsprozess sollte formalisiert und kommuniziert werden, um Maßnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.

Zweck

Es ist sichergestellt, dass das Personal und andere interessierte Parteien die Konsequenzen einer Verletzung der Informationssicherheitsrichtlinien verstehen, um das Personal und andere interessierte Parteien, die eine Verletzung begangen haben, abzuschrecken und angemessen zu behandeln.

Leitfaden

Ein Maßregelungsprozess sollte nicht ohne vorherige Prüfung eingeleitet werden, ob tatsächlich eine Verletzung der Informationssicherheitspolitik aufgetreten ist (siehe 5.28).

Der formale Maßregelungsprozess sollte eine abgestufte Reaktion vorsehen, die Faktoren wie z. B. die folgenden berücksichtigt:

- die Art (wer, was, wann, wie) und die Schwere des Verstoßes und dessen Folgen;
- ob die Straftat vorsätzlich (böswillig) oder unabsichtlich (versehentlich) begangen wurde;
- unabhängig davon, ob es sich um ein erstes oder wiederholtes Vergehen handelt;
- ob die beschuldigte Person geeignet geschult war oder nicht.

Die Reaktion sollte die einschlägigen rechtlichen, gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen sowie gegebenenfalls andere Faktoren berücksichtigen. Ein Maßregelungsprozess sollte auch als Abschreckung dienen, um das Personal und andere interessierte Parteien davon abzuhalten, gegen die Informationssicherheitspolitik, themenspezifische Richtlinien und Verfahren für die Informationssicherheit zu verstoßen. Vorsätzliche Verletzungen der Informationssicherheitsrichtlinien können sofortige Maßnahmen erfordern.

Weitere Informationen

Soweit möglich, sollte die Identität von Personen, gegen die Disziplinarmaßnahmen ergriffen werden, im Einklang mit den geltenden Anforderungen geschützt werden.

Wenn Einzelpersonen ein hervorragendes Verhalten in Bezug auf die Informationssicherheit an den Tag legen, können sie belohnt werden, um die Informationssicherheit zu fördern und gutes Verhalten zu unterstützen.

6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Humanressourcen #Asset_Management	#Governance_und_Ökosystem

Maßnahme

Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.

Zweck

Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung oder von Verträgen.

Leitfaden

Das Verfahren für den Umgang mit der Beendigung oder dem Wechsel des Beschäftigungsverhältnisses sollte festlegen, welche Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit nach der Beendigung oder dem Wechsel bestehen bleiben sollten. Dies kann die Vertraulichkeit von Informationen, geistigem Eigentum und sonstigem erlangten Wissen sowie die in anderen Vertraulichkeitsvereinbarungen enthaltenen Pflichten umfassen (siehe 6.6). Die nach Beendigung des Arbeitsverhältnisses oder des Vertrags weitergeltenden Verantwortlichkeiten und Pflichten sollten in den Beschäftigungsbedingungen (siehe 6.2), dem Vertrag oder der Vereinbarung des Einzelnen beschrieben werden. Auch andere Verträge oder Vereinbarungen, die für einen bestimmten Zeitraum nach Beendigung des Beschäftigungsverhältnisses des Einzelnen weiterbestehen, können Verantwortlichkeiten für die Informationssicherheit enthalten.

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

Die Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit, die eine Person innehat, die ihren Arbeitsplatz verlässt oder wechselt, sollten ermittelt und auf eine andere Person übertragen werden.

Es sollte ein Verfahren für die Mitteilung der Änderungen und der Betriebsverfahren an das Personal, andere interessierte Parteien und relevante Ansprechpartner (z. B. für Kunden und Lieferanten) eingerichtet werden.

Das Verfahren für die Beendigung oder den Wechsel des Beschäftigungsverhältnisses sollte auch auf externes Personal (d. h. Lieferanten) angewandt werden, wenn es zur Kündigung des Personals, des Vertrags oder des Arbeitsplatzes mit der Organisation kommt oder wenn es einen Wechsel des Arbeitsplatzes innerhalb der Organisation gibt.

Weitere Informationen

In vielen Organisationen ist die Personalabteilung im Allgemeinen zuständig für den gesamten Beendigungsprozess und arbeitet mit dem Vorgesetzten der wechselnden Person zusammen, um Aspekte der Informationssicherheit im Zusammenhang mit den entsprechenden Verfahren zu regeln. Falls Personal von einer externen Partei (z. B. über einen Lieferanten) beauftragt wurde, wird dieser Beendigungsprozess von der externen Partei entsprechend dem Vertrag zwischen der Organisation und der externen Partei ausgeführt.

6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Sicherheit_der_Humanressourcen #Informationsschutz #Lieferantenbeziehungen	#Governance_und_Ökosystem

Maßnahme

Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, sollten identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.

Zweck

Wahrung der Vertraulichkeit von Informationen, die dem Personal oder externen Parteien zugänglich sind.

Leitfaden

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 interessierte Parteien oder das Personal der Organisation anwendbar sein. Ausgehend von den Anforderungen einer Organisation an die Informationssicherheit sollten die Bedingungen in den Vereinbarungen unter Berücksichtigung der Art der zu verarbeitenden Informationen, ihrer Klassifizierungsstufe, ihrer Verwendung und des zulässigen Zugriffs durch die andere Partei festgelegt werden. Zur Feststellung der Anforderungen für Vertraulichkeits- oder Geheimhaltungsvereinbarungen sollten die folgenden Elemente in Betracht gezogen werden:

- Definition der zu schützenden Informationen (z. B. vertrauliche Informationen);
- die voraussichtliche Dauer einer Vereinbarung, einschließlich von Fällen, in denen es notwendig sein kann, die Vertraulichkeit auf unbestimmte Zeit oder bis zur öffentlichen Verfügbarkeit der Informationen aufrechtzuerhalten;
- die erforderlichen Maßnahmen bei Beendigung einer Vereinbarung;
- die Pflichten und Maßnahmen der Unterzeichner zur Vermeidung einer unbefugten Offenlegung von Informationen;
- die Eigentümerschaft an Informationen, Geschäftsgeheimnissen und geistigem Eigentum und Zusammenhang mit dem Schutz der vertraulichen Informationen;

- f) die gestattete Nutzung vertraulicher Informationen und Rechte des Unterzeichnenden zur Nutzung der Informationen;
- g) das Recht zur Überprüfung und Überwachung von Aktivitäten, die vertrauliche Informationen berühren, wenn es sich um hochsensible Umstände handelt;
- h) das Verfahren zur Benachrichtigung und Berichterstattung über unbefugte Offenlegung oder Verlust vertraulicher Informationen;
- i) die Bestimmungen bezüglich Informationen, die bei Beendigung der Vereinbarung zurückzugeben bzw. zu vernichten sind;
- j) die Maßnahmen, die im Falle einer Nichteinhaltung der Vereinbarung durchgeführt werden sollen.

Die Organisation sollte die Einhaltung von Vertraulichkeits- und Geheimhaltungsvereinbarungen in dem Land, für das sie gelten, berücksichtigen (siehe 5.31, 5.32, 5.33, 5.34).

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 der 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.

6.7 Telearbeit

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz #Physische_Sicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Es sollten Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.

Zweck

Sicherstellung der Informationssicherheit, wenn das Personal aus der Ferne arbeitet.

Leitfaden

Telearbeit liegt immer dann vor, wenn Mitarbeiter der Organisation von einem Ort außerhalb des Firmengeländes aus arbeiten und dabei auf Informationen in Papierform oder elektronisch über IKT-Geräte zugreifen. Zu den Remote-Arbeitsplätzen gehören die Begriffe „Telearbeit“, „Telecommuting“, „flexibler Arbeitsplatz“, „virtuelle Arbeitsumgebung“ und „Fernwartung“.

ANMERKUNG Es ist möglich, dass nicht alle Empfehlungen in diesem Leitfaden aufgrund lokaler Gesetze und Vorschriften in verschiedenen Ländern angewendet werden können.

Organisationen, die Telearbeit zulassen, sollten eine themenspezifische Richtlinie für Telearbeit erstellen, in der die entsprechenden Bedingungen und Einschränkungen festgelegt sind. Soweit erforderlich, sollten folgende Themen berücksichtigt werden:

- a) die bestehende oder vorgeschlagene physische Sicherheit des Fernarbeitsplatzes unter Berücksichtigung der physischen Sicherheit des Standorts und der örtlichen Umgebung, einschließlich der verschiedenen Rechtsordnungen, in denen sich das Personal befindet;
- b) Regeln und Sicherheitsmechanismen für die entfernte physische Umgebung, wie z. B. abschließbare Aktenschränke, sicherer Transport zwischen den Standorten und Regeln für den Fernzugriff, aufgeräumte Arbeitsumgebung, Ausdrucke und Entsorgung von Informationen und anderen zugehörigen Werten sowie Meldung von Informationssicherheitsvorfällen (siehe 6.8);
- c) die zu erwartenden physischen Telearbeitsumgebungen;
- d) die Sicherheitsanforderungen für die Kommunikation, unter Berücksichtigung des notwendigen Fernzugriffs auf organisationseigene Systeme, die Sensibilität der Information auf die zugegriffen und die über Telekommunikationsverbindungen weitergegeben wird sowie die Empfindlichkeit der Systeme und Anwendungen;
- e) die Nutzung des Fernzugriffs, z. B. des virtuellen Desktop-Zugriffs, der die Verarbeitung und Speicherung von Informationen auf privaten Geräten unterstützt;
- f) die Gefahr des unbefugten Zugriffs auf Information durch andere Personen am Telearbeitsplatz, (z. B. Familie und Freunde);
- g) die Gefahr des unbefugten Zugriffs auf Information durch andere Personen an öffentlichen Orten;
- h) die Verwendung von Heimnetzwerken und öffentlichen Netzen sowie Anforderungen und Beschränkungen der Konfiguration von drahtlosen Netzwerkdiensten;
- i) Einsatz von Sicherheitsmaßnahmen wie Firewalls und Schutz vor Schadsoftware;
- j) sichere Mechanismen für die Bereitstellung und Initialisierung von Systemen aus der Ferne;
- k) sichere Mechanismen für die Authentifizierung und die Freigabe von Zugriffsrechten unter Berücksichtigung der Anfälligkeit von Ein-Faktor-Authentifizierungsmechanismen, wenn der Fernzugriff auf das Netzwerk der Organisation erlaubt ist.

Die zu berücksichtigenden Richtlinien und Maßnahmen sollten enthalten:

- a) die Bereitstellung geeigneter Geräte und Aufbewahrungsmöbel für Telearbeitstätigkeiten, dort wo der Einsatz von privaten, nicht unter der Aufsicht der Organisation stehenden Geräten untersagt ist;
- b) die Festlegung gestatteter Arbeit, die Klassifizierung der Informationen, die aufbewahrt werden können, und die internen Systeme und Dienste, auf die der Telearbeiter berechtigten Zugriff hat;
- c) die Bereitstellung von Schulungsmaßnahmen für die Mitarbeiter, die aus der Ferne arbeiten, und für diejenigen, die sie unterstützen. Dazu gehört auch, wie man bei der Arbeit aus der Ferne sicher vorgeht;
- d) die Bereitstellung geeigneter Kommunikationsgeräte, einschließlich Verfahren zur Sicherung des Fernzugriffs, z. B. Anforderungen an Bildschirmsperren und Inaktivitätstimer; die Ermöglichung der Geräteortung; die Einrichtung von Fernlöschfunktionen;

- e) physische Sicherheit;
- f) Regeln und Leitfäden für den Zugang von Familie und Besuchern zu Geräten und Informationen;
- g) die Bereitstellung von Hard- und Software Support und Wartung;
- h) Bereitstellung von Versicherungen;
- i) Verfahren für Backups und Business Continuity;
- j) Auditierung und Überwachung der Sicherheit;
- k) Widerruf von Befugnissen und Zugriffsrechten sowie die Rückgabe von Geräten wenn die Telearbeitstätigkeiten beendet sind.

Weitere Informationen

Keine weiteren Informationen.

6.8 Meldung von Informationssicherheitsereignissen

Maßnahmenart	Informationssicherheits-eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen	#Handhabung_von_Informationssicherheitsereignissen	#Verteidigung

Maßnahme

Die Organisation sollte einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.

Zweck

Unterstützung der rechtzeitigen, konsistenten und effektiven Meldung von Informationssicherheitsereignissen, die vom Personal identifiziert werden können.

Leitfaden

Alle Mitarbeiter und Benutzer sollten auf ihre Verantwortung hingewiesen werden, Informationssicherheitsereignisse so schnell wie möglich zu melden, um die Auswirkungen von Vorfällen im Bereich der Informationssicherheit zu verhindern oder zu minimieren. Sie sollten das Verfahren zur Meldung über Informationssicherheitsereignisse kennen sowie den Ansprechpartner, an den die Ereignisse zu berichten sind. Der Meldevorgang sollte so einfach, zugänglich und verfügbar wie möglich gehalten werden. Zu den Ereignissen der Informationssicherheit gehören Vorfälle, Verstöße und Schwachstellen.

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

- a) ineffektive Maßnahmen zur Informationssicherheit;
- b) Verstöße gegen die erwartete Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen;

- c) menschliches Versagen;
- d) Nichteinhaltung der Informationssicherheitspolitik, themenspezifischer Richtlinien oder geltender Normen;
- e) Verstöße gegen physische Sicherheitsmaßnahmen;
- f) Systemänderungen, die nicht den Änderungsmanagementprozess durchlaufen haben;
- g) Fehlfunktionen oder anderes anormales Systemverhalten von Software oder Hardware;
- h) Zugangsverstöße;
- i) Schwachstellen;
- j) vermutete Infektion der Schadsoftware.

Mitarbeitern und Benutzern sollte abgeraten werden, einen Versuch zum Nachweis der vermuteten Informationssicherheitsschwachstellen zu unternehmen. Das Austesten von Schwachstellen kann als potentielle Fehlanwendung des Systems interpretiert werden und zudem zu Schäden am Informationssystem oder Diensten führen sowie digitale Beweise beschädigen oder unkenntlich machen. Letztendlich kann dies eine rechtliche Haftung der ausführenden Person nach sich ziehen.

Weitere Informationen

Der Normenreihe ISO/IEC 27035 sind zusätzliche Informationen zu entnehmen.

7 Physische Maßnahmen

7.1 Physische Sicherheitsperimeter

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz

Maßnahme

Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, sollten Sicherheitsperimeter festgelegt und verwendet werden.

Zweck

Verhinderung des unbefugten physischen Zugriffs, der Beschädigung und des Eingriffs in die Informationen der Organisation und anderer zugehöriger Werte.

Leitfaden

Die folgenden Richtlinien sollten in physischen Sicherheitsperimetern in Betracht gezogen und ggf. umgesetzt werden:

- a) Festlegung von Sicherheitsperimetern und der Lage und Stärke jedes einzelnen Perimeters in Übereinstimmung mit den Informationssicherheitsanforderungen für die Werte innerhalb des Perimeters;
- b) physisch solide Perimeter für ein Gebäude oder ein Gelände, das Einrichtungen zur Informationsverarbeitung enthält (d. h. es sollten keine Lücken in den Perimetern oder Bereichen vorhanden sein, in die leicht eingebrochen werden kann). Die Außendächer, -wände, -decken und -böden des Geländes sollten aus einer soliden Konstruktion bestehen, und alle Außentüren sollten in geeigneter Weise durch Kontrollmechanismen (z. B. Gitter, Alarmanlagen, Schlösser) gegen unbefugten Zugang geschützt sein. Türen und Fenster sollten verschlossen werden, wenn sie unbeaufsichtigt sind, und es sollte ein Außenschutz für die Fenster, insbesondere im Erdgeschoss, in Betracht gezogen werden; außerdem sollten Lüftungspunkte berücksichtigt werden;
- c) Alarmierung, Überwachung und Prüfung aller Brandschutztüren in einem Sicherheitsperimeter in Verbindung mit den Wänden, um den erforderlichen Widerstandsgrad nach geeigneten Normen zu ermitteln. Sie sollten ausfallsicher arbeiten.

Weitere Informationen

Ein physischer Schutz kann durch Errichtung einer oder mehrerer physischer Barrieren rund um das Gelände der Organisation und die Einrichtungen zur Informationsverarbeitung erreicht werden.

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 Perimeter zur Kontrolle des physischen Zugangs können erforderlich sein zwischen Bereichen mit unterschiedlichen Sicherheitsanforderungen innerhalb der Sicherheitsperimeter. Die Organisation sollte physische Sicherheitsmaßnahmen in Erwägung ziehen, die in Situationen erhöhter Bedrohung verstärkt werden können.

7.2 Physischer Zutritt

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.

Zweck

Sicherstellung, dass nur autorisierter physischer Zugang zu den Informationen der Organisation und anderen zugehörigen Werten erfolgt.

Leitfaden

Allgemeines

Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten können, sollten überwacht und, falls möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unbefugten Zutritt zu verhindern.

Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- a) Beschränkung des Zugangs zu Grundstücken und Gebäuden auf befugtes Personal. Das Verfahren für die Verwaltung der Zugangsrechte zu physischen Bereichen sollte die Erteilung, die regelmäßige Überprüfung, die Aktualisierung und den Widerruf von Genehmigungen umfassen (siehe 5.18);
- b) sicheres Führen und Überwachen eines physischen Logbuchs oder eines elektronischen Prüfpfads aller Zugriffe und Schutz aller Protokolle (siehe 5.33) und sensiblen Authentifizierungsinformationen;
- c) Einführung und Umsetzung eines Verfahrens und technischer Mechanismen für die Verwaltung des Zugangs zu Bereichen, in denen Informationen verarbeitet oder gespeichert werden. Zu den Authentifizierungsmechanismen gehören die Verwendung von Zugangskarten, biometrische Verfahren oder die Zwei-Faktor-Authentifizierung, z. B. mit einer Zugangskarte und einer geheimen PIN. Für den Zugang zu sensiblen Bereichen sollten doppelte Sicherheitstüren in Betracht gezogen werden;
- d) Einrichtung eines von Personal überwachten Empfangsbereichs oder andere Mittel zur Kontrolle des physischen Zugangs zum Gelände oder Gebäude;
- e) Kontrolle und Überprüfung der persönlichen Gegenstände des Personals und der interessierten Parteien beim Betreten und Verlassen;

ANMERKUNG Für die mögliche Kontrolle von persönlichen Gegenständen können örtliche Gesetze und Vorschriften bestehen.

- f) Verpflichtung für alle Mitarbeiter und interessierte Parteien, 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. Zur besseren Identifizierung von Festangestellten, Lieferanten und Besuchern sollten leicht erkennbare Ausweise in Betracht gezogen werden;
- g) Gewährung von eingeschränktem Zugang zu Sicherheitsbereichen oder Informationsverarbeitungseinrichtungen für das Personal des Lieferanten nur bei Bedarf. Dieser Zugang sollte genehmigt und überwacht werden;
- h) besondere Aufmerksamkeit hinsichtlich der Sicherung des physischen Zugangs zu Gebäuden, in denen sich Werte mehrerer Organisationen befinden;
- i) Gestaltung der physischen Sicherheitsmaßnahmen, damit sie verstärkt werden können, wenn die Wahrscheinlichkeit physischer Vorfälle steigt;
- j) Sicherung anderer Zugangspunkte wie Fluchtwege und Notausgänge vor unbefugtem Zutritt;
- k) Einrichtung eines Schlüsselverwaltungsprozesses, um die Verwaltung der physischen Schlüssel oder Authentifizierungsinformationen (z. B. Schlosscodes, Kombinationsschlösser für Büros, Räume und Einrichtungen wie Schlüsselschränke) sicherzustellen und ein Logbuch oder ein jährliches Schlüsselaudit sicherzustellen und zu gewährleisten, dass der Zugang zu physischen Schlüsseln oder Authentifizierungsinformationen kontrolliert wird (siehe 5.17 für weitere Hinweise zu Authentifizierungsinformationen).

Besucher

Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- a) Authentifizierung der Identität der Besucher durch ein geeignetes Mittel;
- b) Aufzeichnung von Datum und Uhrzeit der Ein- und Austrittszeit der Besucher;
- c) Gewährung des Zugangs für Besucher nur für bestimmte, genehmigte Zwecke und mit Anweisungen zu den Sicherheitsanforderungen des Bereichs und zu den Notfallverfahren;
- d) Beaufsichtigung aller Besucher, es sei denn, es wird eine ausdrückliche Ausnahme gewährt.

Anlieferungs- und Ladebereiche und eingehendes Material

Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- a) Beschränkung des Zutritts zu Anlieferungs- und Ladebereichen von außerhalb des Gebäudes für identifizierte und befugte Beschäftigte;
- b) Gestaltung der Anlieferungs- und Ladebereiche, so dass Lieferungen beladen und entladen werden können, ohne dass das Lieferpersonal unbefugten Zutritt zu anderen Teilen des Gebäudes erhält;
- c) Sicherung der Außentüren von Liefer- und Verladebereichen, wenn die Türen zu Sperrbereichen geöffnet werden;
- d) Prüfung und Untersuchung eingehender Lieferungen auf Sprengstoffe, Chemikalien oder andere Gefahrstoffe, bevor sie aus den Anlieferungs- und Ladebereichen entfernt werden;
- e) Registrierung der eingehenden Lieferungen entsprechend der Verfahren zur Verwaltung der Werte (siehe 5.9 und 7.10) beim Eingang am Standort;
- f) physische Trennung eingehender und ausgehender Lieferungen, soweit möglich;
- g) Prüfung der eingehenden Lieferungen auf Anzeichen von Manipulationen unterwegs. Sofern sich Anzeichen für Manipulationen finden, sollten diese unverzüglich dem Sicherheitspersonal gemeldet werden.

Weitere Informationen

Keine weiteren Informationen.

7.3 Sichern von Büros, Räumen und Einrichtungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz

Maßnahme

Die physische Sicherheit für Büros, Räume und Einrichtungen sollte konzipiert und umgesetzt werden.

Zweck

Verhinderung des unbefugten physischen Zugriffs, der Beschädigung und des Eingriffs in die Informationen der Organisation und anderer zugehöriger Werte in Büros, Räumen und Einrichtungen.

Leitfaden

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

- Standortwahl für kritische Einrichtungen, um den Zugang der Öffentlichkeit zu vermeiden;
- gegebenenfalls Sicherstellung, dass die Gebäude 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;
- Konfiguration von Einrichtungen, so dass von außen keine vertraulichen Informationen oder Aktivitäten zu sehen oder zu hören sind. Gegebenenfalls sollte auch eine elektromagnetische Abschirmung in Betracht gezogen werden;
- Verzeichnisse, interne Telefonbücher und online zugängliche Karten, auf denen die Standorte von Einrichtungen zur Verarbeitung vertraulicher Informationen verzeichnet sind, dürfen Unbefugten nicht ohne weiteres zugänglich gemacht werden.

Weitere Informationen

Keine weiteren Informationen.

7.4 Physische Sicherheitsüberwachung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Erkennen	#Physische_Sicherheit	#Schutz #Verteidigung

Maßnahme

Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.

Zweck

Erkennen und Abschrecken von unbefugtem physischen Zutritt.

Leitfaden

Die physischen Räumlichkeiten sollten durch Überwachungssysteme überwacht werden, zu denen Wachpersonal, Einbruchalarm, Videoüberwachungssysteme wie z. B. Videoinspektionssysteme und Software für das Informationsmanagement im Bereich der physischen Sicherheit gehören können, die entweder intern oder von einem Überwachungsdienstleister verwaltet werden.

Der Zutritt zu Gebäuden, in denen sich kritische Systeme befinden, sollte ständig überwacht werden, um unbefugten Zutritt oder verdächtiges Verhalten von Personen zu erkennen:

- a) die Installation von Videoüberwachungssystemen, wie z. B. Videoinspektionssystem, um den Zutritt zu sensiblen Bereichen innerhalb und außerhalb der Räumlichkeiten einer Organisation zu überwachen und aufzuzeichnen;
- b) Installation von Kontakt-, Schall- oder Bewegungsmeldern, die einen Einbruchalarm auslösen, nach den einschlägigen geltenden Normen und deren regelmäßige Prüfung, z. B.:
 - 1) Installation von Kontaktmeldern, die bei Kontaktaufnahme oder -unterbrechung einen Alarm auslösen, an allen Stellen, an denen ein Kontakt hergestellt oder unterbrochen werden kann (z. B. an Fenstern, Türen und unter Gegenständen), um als Panikalarm zu dienen;
 - 2) Bewegungsmelder auf Infrarotbasis, die einen Alarm auslösen, wenn ein Objekt durch ihr Sichtfeld läuft;
 - 3) Installation von Sensoren, die auf das Geräusch von zerbrechendem Glas reagieren und so einen Alarm auslösen können, um das Sicherheitspersonal zu alarmieren;
- c) Verwendung dieser Alarme für alle Außentüren und zugänglichen Fenster. Unbesetzte Räume sollten stets alarmgesichert sein; auch für andere Bereiche (z. B. Computer- oder Kommunikationsräume) sollte ein Schutz vorgesehen werden.

Die Konzeption von Überwachungssystemen sollte vertraulich behandelt werden, da eine Offenlegung unentdeckte Einbrüche erleichtern kann.

Überwachungssysteme sollten vor unbefugtem Zutritt geschützt werden, um zu verhindern, dass Unbefugte auf Überwachungsdaten, wie z. B. Videobilder, zugreifen oder Systeme aus der Ferne deaktiviert werden können.

Die Zentrale der Alarmanlage sollte sich in einem alarmgesicherten Bereich und bei Sicherheitsalarmen an einem Ort befinden, der der Person, die den Alarm auslöst, einen einfachen Fluchtweg ermöglicht. Die Schalttafel und die Melder sollten über manipulationssichere Mechanismen verfügen. Das System sollte regelmäßig geprüft werden, um sicherzustellen, dass es wie vorgesehen funktioniert, insbesondere wenn seine Komponenten batteriebetrieben sind.

Alle Überwachungs- und Aufzeichnungsmechanismen sollten unter Berücksichtigung der örtlichen Gesetze und Vorschriften, einschließlich der Gesetze zum Datenschutz und zum Schutz personenbezogener Daten, eingesetzt werden, insbesondere im Hinblick auf die Überwachung des Personals und die Aufbewahrungsfristen für Videoaufzeichnungen.

Weitere Informationen

Keine weiteren Informationen.

7.5 Schutz vor physischen und umweltbedingten Bedrohungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz

Maßnahme

Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur sollte geplant und umgesetzt werden.

Zweck

Verhinderung oder Verringerung der Folgen von Ereignissen, die auf physische und umweltbedingte Bedrohungen zurückzuführen sind.

Leitfaden

Risikobeurteilungen zur Ermittlung der potentiellen Folgen von physischen und umweltbedingten Bedrohungen sollten vor der Aufnahme kritischer Vorgänge an einem physischen Standort und in regelmäßigen Abständen durchgeführt werden. Es sollten die erforderlichen Schutzmaßnahmen ergriffen und Änderungen der Bedrohungen überwacht werden. Es sollte fachkundiger Rat eingeholt werden, wie mit Risiken umzugehen ist, die sich aus physischen und umweltbedingten Bedrohungen wie Feuer, Überschwemmungen, Erdbeben, Explosionen, zivilen Unruhen, Giftmüll, Umweltemissionen und anderen Formen von Naturkatastrophen oder von Menschen verursachten Katastrophen ergeben.

Bei der Wahl des Standorts und der Konstruktion der Räumlichkeiten sollte Folgendes berücksichtigt werden:

- a) die örtliche Topographie, z. B. geeignete Höhenlagen, Gewässer und tektonische Verwerfungen;
- b) urbane Bedrohungen, z. B. Orte, die für politische Unruhen, kriminelle Aktivitäten oder Terroranschläge bekannt sind.

Auf der Grundlage der Ergebnisse der Risikobeurteilung sollten relevante physische und umweltbedingte Bedrohungen identifiziert und geeignete Maßnahmen erwogen werden, z. B. in den folgenden Bereichen:

- a) Feuer: Installation und Konfiguration von Systemen zur frühzeitigen Erkennung von Bränden und zur Auslösung von Alarmen oder Brandbekämpfungssystemen, um Brandschäden an Speichermedien und den dazugehörigen Informationsverarbeitungssystemen zu verhindern. Die Brandbekämpfung sollte mit dem für die Umgebung am besten geeigneten Mittel durchgeführt werden (z. B. Gas in geschlossenen Räumen);
- b) Überschwemmung: Installation von Systemen zur frühzeitigen Erkennung von Überschwemmungen unter den Böden von Räumen, in denen sich Speichermedien oder Informationsverarbeitungssysteme befinden. Für den Fall einer Überschwemmung sollten Wasserpumpen oder gleichwertige Mittel bereitstehen;
- c) Überspannungen: Einführung von Systemen, die sowohl Server- als auch Client-Informationssysteme vor Überspannungen oder ähnlichen Ereignissen schützen können, um die Folgen solcher Ereignisse zu minimieren;
- d) Sprengstoffe und Waffen: Durchführung von Stichprobenkontrollen auf das Vorhandensein von Sprengstoffen oder Waffen bei Personen, Fahrzeugen oder Waren, die in sensible Informationsverarbeitungseinrichtungen gelangen.

Weitere Informationen

Safes und andere Formen sicherer Lagerungseinrichtungen können außerdem dorthin verbrachte Informationen vor Katastrophen wie Bränden, Erdbeben, Überschwemmungen oder Explosionen schützen.

Organisationen können die Konzepte der Verbrechensverhütung durch Umweltgestaltung berücksichtigen, wenn sie die Maßnahmen zur Sicherung ihrer Umgebung und zur Verringerung der Bedrohungen in den Städten planen. Anstelle von Pollern können zum Beispiel Statuen oder Wasserspiele sowohl als Merkmal als auch als physische Barriere dienen.

7.6 Arbeiten in Sicherheitsbereichen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz

Maßnahme

Es sollten Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.

Zweck

Schutz von Informationen und anderen zugehörigen Werten in Sicherheitsbereichen vor Beschädigung und unbefugten Eingriffen durch Personal, das in diesen Bereichen arbeitet.

Leitfaden

Die Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen sollten für das gesamte Personal gelten und alle Tätigkeiten abdecken, die in dem Sicherheitsbereich stattfinden.

Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- a) Benachrichtigung des Personals über das Vorhandensein oder die Aktivitäten in einem Sicherheitsbereich nur auf der Grundlage des Wissensbedarfs;
- b) Vermeidung unbeaufsichtigter Arbeiten in Sicherheitsbereichen sowohl aus Sicherheitsgründen als auch zur Verringerung des Risikos bössartiger Aktivitäten;
- c) physische Verriegelung und regelmäßige Inspektion leerstehender Sicherheitsbereiche;
- d) das Untersagen von Foto-, Video-, Audio- oder sonstigen Aufzeichnungsgeräten, wie z. B. Kameras in Benutzerendgeräten und Gestattung nur nach ausdrücklicher Genehmigung;
- e) die angemessene Kontrolle des Mitführens und der Verwendung von Endgeräten in Sicherheitsbereichen;
- f) Aushang von Notfallmaßnahmen in gut sichtbarer oder zugänglicher Weise.

Weitere Informationen

Keine weiteren Informationen.

7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Physische_Sicherheit	#Schutz

Maßnahme

Es sollten klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.

Zweck

Verringerung des Risikos des unbefugten Zutritts, des Verlusts und der Beschädigung von Informationen auf Schreibtischen, Bildschirmen und an anderen zugänglichen Orten während und außerhalb der normalen Arbeitszeiten.

Leitfaden

Die Organisation sollte eine themenspezifische Richtlinie zur aufgeräumten Arbeitsumgebung und zu Bildschirmsperren einführen und allen relevanten interessierten Parteien mitteilen.

Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- Aufbewahrung sensibler oder geschäftskritischer Informationen (z. B. auf Papier oder elektronischen Speichermedien) (idealerweise in einem Tresor, Schrank oder anderen Sicherheitsmöbeln), wenn sie nicht benötigt werden, insbesondere wenn das Büro nicht besetzt ist;
- Schutz der Endpunktgeräte der Benutzer durch Schlüsselsperren oder andere Sicherheitsvorkehrungen, wenn sie nicht benutzt werden oder unbeaufsichtigt sind;
- Abmeldung der Endpunktgeräte des Benutzers oder Schutz durch einen Bildschirm- und Tastatursperrmechanismus, der durch einen Benutzerauthentifizierungsmechanismus gesteuert wird, wenn sie unbeaufsichtigt sind. Alle Computer und Systeme sollten mit einer Timeout- oder automatischen Logout-Funktion ausgestattet sein;
- der Urheber wird dazu veranlasst, die Ausgaben von Druckern oder Multifunktionsgeräten sofort zu erfassen. Die Nutzung von Druckern mit Authentifizierungsfunktion sollte in Betracht gezogen werden, um sicherzustellen, dass nur die jeweiligen Urheber ihre Ausdrücke erhalten können und nur dann, wenn sie neben dem Drucker stehen;
- sichere Aufbewahrung von Dokumenten und Wechseldatenträgern mit sensiblen Informationen und, wenn sie nicht mehr benötigt werden, deren Entsorgung unter Verwendung sicherer Entsorgungsmechanismen;
- Festlegung und Bekanntgabe von Regeln und Leitlinien für die Konfiguration von Pop-up-Fenstern auf Bildschirmen (z. B. Deaktivierung der neuen E-Mail- und Nachrichten-Pop-ups, wenn möglich, bei Präsentationen, gemeinsamer Bildschirmnutzung oder in einem öffentlichen Bereich);
- Löschen von sensiblen oder kritischen Informationen auf Whiteboards und anderen Anzeigegeräten, wenn sie nicht mehr benötigt werden.

Die Organisation sollte über Verfahren für die Räumung von Einrichtungen verfügen, einschließlich der Durchführung einer abschließenden Durchsuchung vor dem Verlassen, um sicherzustellen, dass die Werte der Organisation nicht zurückgelassen werden (z. B. Dokumente, die in Schubladen oder Möbeln liegen).

Weitere Informationen

Keine weiteren Informationen.

7.8 Platzierung und Schutz von Geräten und Betriebsmitteln

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz

Maßnahme

Die Geräte und Betriebsmittel sollten sicher und geschützt aufgestellt werden.

Zweck

Verringerung der Risiken durch physische und umweltbedingte Bedrohungen sowie durch unbefugten Zugang und Beschädigung.

Leitfaden

Zum Schutz von Geräten und Betriebsmitteln sollten die folgenden Richtlinien berücksichtigt werden:

- Platzierung der Ausrüstung, um unnötigen Zutritt zu Arbeitsbereichen zu minimieren und unbefugten Zutritt zu vermeiden;
- sorgfältige Wahl des Standorts von Einrichtungen zur Informationsverarbeitung, in denen mit sensiblen Daten umgegangen wird, zur Verringerung des Risikos, dass unbefugte Personen während der Verarbeitung Einblick in die Informationen erhalten;
- Einführung von Maßnahmen, 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 Telekommunikations-einrichtungen, elektromagnetische Strahlung und Vandalismus möglichst gering zu halten;
- Aufstellung von Leitlinien für das Essen, Trinken und Rauchen in der Nähe von Einrichtungen zur Informationsverarbeitung;
- Überwachung von Umweltbedingungen wie Temperatur und Luftfeuchtigkeit auf Bedingungen, die den Betrieb der Einrichtungen zur Informationsverarbeitung beeinträchtigen können;
- Anbringung eines Blitzschutzes an allen Gebäuden und Einbau von Blitzschutzfiltern in alle eingehenden Strom- und Telekommunikationsleitungen;
- Erwägung des Einsatzes besonderer Schutzmaßnahmen, wie z. B. Folientastaturen, für Geräte in industriellen Umgebungen;

- h) Schutz von Geräten, in denen vertrauliche Informationen verarbeitet werden, zur Minimierung des Risikos von Informationsverlusten aufgrund elektromagnetischer Abstrahlung;
- i) physische Trennung der von der Organisation verwalteten Informationsverarbeitungseinrichtungen von denen, die nicht von der Organisation verwaltet werden.

Weitere Informationen

Keine weiteren Informationen.

7.9 Sicherheit von Werten außerhalb der Räumlichkeiten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz

Maßnahme

Werte außerhalb des Standorts sollten geschützt werden.

Zweck

Verlust, Beschädigung, Diebstahl oder Gefährdung von Geräten außerhalb des Standorts und die Unterbrechung von Organisationstätigkeiten sind unterbunden.

Leitfaden

Jedes Gerät, das außerhalb der Räumlichkeiten der Organisation verwendet wird und Informationen speichert oder verarbeitet (z. B. ein mobiles Gerät), einschließlich der Geräte, die sich im Besitz der Organisation befinden, und der Geräte, die sich im Privatbesitz befinden und im Auftrag der Organisation verwendet werden [Bring your own device (BYOD)], muss geschützt werden. Die Verwendung dieser Geräte sollte vom Management genehmigt werden.

Die folgenden Leitlinien sollten für den Schutz von Geräten berücksichtigt werden, die Informationen außerhalb der Räumlichkeiten der Organisation speichern oder verarbeiten:

- a) keine Geräte und Speichermedien, die aus den Räumlichkeiten mitgenommen werden, unbeaufsichtigt an öffentlichen und ungesicherten Orten zurücklassen;
- b) ständige Beachtung der Herstelleranweisungen zum Schutz der Geräte und Betriebsmittel (z. B. Schutz vor starken elektromagnetischen Feldern, Wasser, Hitze, Feuchtigkeit, Staub);
- c) wenn Betriebsmittel außerhalb des Betriebsgeländes zwischen verschiedenen Personen oder interessierten Parteien weitergegeben werden, die ein Protokoll führen, in dem die Kontrollkette für die Betriebsmittel einschließlich mindestens der Namen und Organisationen der für die Betriebsmittel Verantwortlichen festgehalten werden. Informationen, die nicht mit dem Wert übertragen werden müssen, sollten vor der Übertragung sicher gelöscht werden;
- d) sofern notwendig und praktikabel, Einholung einer Genehmigung für die Entfernung von Geräten und Datenträgern aus den Räumlichkeiten der Organisation und Führung von Aufzeichnungen über solche Entfernungen, um einen Prüfpfad aufrechtzuerhalten (siehe 5.14);

- e) Schutz vor der Einsichtnahme in Informationen auf einem Gerät (z. B. Handy oder Laptop) in öffentlichen Verkehrsmitteln und vor den mit dem „Schulter-Surfen“ verbundenen Risiken;
- f) Umsetzung der Standortverfolgung und Möglichkeit der Fernlöschung von Geräten.

Die dauerhafte Installation von Geräten außerhalb des Organisationsgeländes [wie z. B. Antennen und Geldautomaten] kann einem höheren Risiko der Beschädigung, des Diebstahls oder des Abhörens ausgesetzt sein. Diese Risiken können an verschiedenen Orten sehr unterschiedlich stark ausgeprägt sein und sollten bei der Bestimmung der am besten geeigneten Maßnahmen in Betracht gezogen werden. Die folgenden Leitlinien sollten berücksichtigt werden, wenn diese Geräte außerhalb des Geländes der Organisation aufgestellt werden:

- a) physische Sicherheitsüberwachung (siehe 7.4);
- b) Schutz vor physischen und umweltbedingten Bedrohungen (siehe 7.5);
- c) physischer Zugang und manipulationssichere Maßnahmen;
- d) logische Zugangssteuerung.

Weitere Informationen

Weitere Informationen zu anderen Aspekten des Schutzes von Informationsspeicher- und -verarbeitungsgeräten und Endpunktgeräten der Benutzer können 8.1 und 6.7 entnommen werden.

7.10 Speichermedien

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz

Maßnahme

Speichermedien sollten während ihres gesamten Lebenszyklus - Erwerb, Verwendung, Transport und Entsorgung - in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.

Zweck

Es wird sichergestellt, dass Informationen auf Speichermedien nur mit Genehmigung offengelegt, verändert, entfernt oder zerstört werden.

Leitfaden

Wechselspeichermedien

Die folgenden Leitlinien für die Handhabung von Wechselspeichermedien sollten beachtet werden:

- a) Festlegung einer themenspezifischen Richtlinie für die Verwaltung von Wechselspeichermedien und Weitergabe dieser themenspezifischen Richtlinie an alle, die Wechselspeichermedien verwenden oder damit umgehen;

- b) sofern notwendig und praktikabel ist, Einholung einer Genehmigung für die Entfernung von Speichermedien aus der Organisation und Führung von Aufzeichnungen über solche Entfernungen, um einen Prüfpfad aufrechtzuerhalten;
- c) Aufbewahrung aller Speichermedien in einer sicheren Umgebung entsprechend ihrer Informationsklassifizierung und Schutz vor umweltbezogenen Bedrohungen (wie z. B. Hitze, Feuchte, Luftfeuchte, elektronische Felder oder Alterung) in Übereinstimmung mit den Herstellerspezifikationen;
- d) wenn die Vertraulichkeit oder Integrität der Informationen wichtige Gesichtspunkte darstellen, sollten kryptographische Techniken zum Schutz von Informationen auf Wechseldatenträgern eingesetzt werden;
- e) um das Risiko zu mindern, dass Speichermedien beschädigt werden, während die gespeicherten Informationen noch benötigt werden, und dass die Informationen auf neue Speichermedien übertragen werden, bevor sie unlesbar werden;
- f) Speicherung mehrerer Kopien wertvoller Informationen auf separaten Speichermedien, um das Risiko einer zufälligen Beschädigung oder eines Verlusts von Informationen weiter zu verringern;
- g) Erwägung der Registrierung von Wechselspeichermedien, um das Risiko eines Informationsverlustes zu verringern;
- h) Aktivierung von Anschlüssen für Wechseldatenträger [z. B. Secure Digital (SD)-Kartensteckplätze und Universal Serial Bus (USB)-Anschlüsse] nur, wenn es einen organisatorischen Grund für ihre Verwendung gibt;
- i) falls eine Notwendigkeit zur Verwendung von Wechseldatenträgern besteht, Überwachung der Übertragung von Informationen auf solche Speichermedien;
- j) Informationen können einem unberechtigten Zugriff, einer Fehlanwendung oder einer Verfälschung während des Transports ausgesetzt sein, wenn Speichermedien z. B. über einen Postdienstleister oder per Kurier versandt werden.

Im Rahmen dieser Maßnahme gehören zu den Datenträgern auch Papierdokumente. Bei der Übertragung von physischen Speichermedien sind die Sicherheitsmaßnahmen nach 5.14 anzuwenden.

Sichere Wiederverwendung oder Entsorgung

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

- a) wenn Speichermedien mit vertraulichen Informationen innerhalb der Organisation wiederverwendet werden müssen, sichere Löschung der Daten oder Formatierung der Speichermedien vor der Wiederverwendung (siehe 8.10);
- b) sichere Entsorgung von Speichermedien mit vertraulichen Informationen, wenn diese nicht mehr benötigt werden (z. B. durch Vernichtung, Schreddern oder sicheres Löschen des Inhalts);
- c) vorhandene Verfahren zur Ermittlung von Daten, bei denen eine derartige Entsorgung erforderlich sein kann;
- d) viele Organisationen bieten Abhol- und Entsorgungsdienste für Speichermedien an. Die Auswahl eines geeigneten externen Dienstleisters sollte mit Bedacht und unter der Voraussetzung erfolgen, dass dieser angemessene Sicherheitsmaßnahmen und Erfahrung vorweisen kann;

- e) Protokollierung der Entsorgung von Datenträgern mit sensiblen Daten, um einen Prüfpfad aufrechtzuerhalten;
- f) bei der Anhäufung von Speichermedien, die entsorgt werden sollen unter Berücksichtigung des Kumulierungseffekts, der dazu führen kann, dass eine große Menge einzeln nicht sensibler Information zusammengekommen einen Bestand sensibler Information darstellen kann.

Bei beschädigten Geräten, die sensible Daten enthalten, sollte eine Risikobeurteilung durchgeführt werden,, um zu bestimmen, ob diese Datenträger physisch zerstört, zur Reparatur versandt oder anderweitig ausgesondert werden sollten (siehe 7.14).

Weitere Informationen

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

7.11 Versorgungseinrichtungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Detektiv	#Integrität #Verfügbarkeit	#Schützen #Erkennen	#Physische_Sicherheit	#Schutz

Maßnahme

Informationsverarbeitungseinrichtungen sollten vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.

Zweck

Verhinderung des Verlusts, der Beschädigung oder der Gefährdung von Informationen und anderen zugehörigen Werten oder der Unterbrechung der Betriebsabläufe der Organisation aufgrund von Ausfällen und Störungen der unterstützenden Versorgungseinrichtungen.

Leitfaden

Organisationen sind auf Versorgungseinrichtungen (z. B. Strom, Telekommunikation, Wasserversorgung, Gas, Abwasser, Belüftung und Klimatisierung) angewiesen, um ihre Informationsverarbeitungseinrichtungen zu unterstützen. Daher sollte die Organisation:

- a) sicherstellen, dass die Geräte, die die Versorgungseinrichtungen unterstützen, in Übereinstimmung mit den jeweiligen Herstellerspezifikationen konfiguriert, betrieben und gewartet werden;
- b) sicherstellen, dass Versorgungseinrichtungen regelmäßig auf ihre ausreichende Auslegung hinsichtlich steigender geschäftlicher Anforderungen sowie ihrer Interaktion mit den anderen Versorgungseinrichtungen begutachtet werden;
- c) sicherstellen, dass die Geräte zur Unterstützung der Versorgungseinrichtungen regelmäßig untersucht und geprüft werden, um ihre ordnungsgemäße Funktion sicherzustellen;
- d) bei Bedarf Alarmer auslösen, damit Fehlfunktionen der Versorgungseinrichtungen schnell erkannt werden;

- e) bei Bedarf sicherstellen, dass mehrere Zuführungen über unterschiedliche Zuleitungswege verfügen;
- f) sicherstellen, dass die Geräte zur Unterstützung der Versorgungseinrichtungen in einem von den Informationsverarbeitungseinrichtungen getrennten Netz betrieben werden, falls sie an ein Netz angeschlossen sind;
- g) sicherstellen, dass die Geräte zur Unterstützung der Versorgungseinrichtungen nur bei Bedarf und nur auf sichere Weise mit dem Internet verbunden sind.

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. Die Kontaktdaten für den Notfall sollten aufgezeichnet werden und dem Personal im Falle eines Ausfalls zur Verfügung stehen.

Weitere Informationen

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

7.12 Sicherheit der Verkabelung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz

Maßnahme

Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, sollten vor Unterbrechung, Störung oder Beschädigung geschützt werden.

Zweck

Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Gefährdung von Informationen und anderen zugehörigen Werten oder der Unterbrechung der Betriebsabläufe der Organisation im Zusammenhang mit der Strom- und Kommunikationsverkabelung.

Leitfaden

Die folgenden Richtlinien zur Verkabelung sollten dabei berücksichtigt werden:

- a) Strom- und Telekommunikationsleitungen, die in Informationsverarbeitungseinrichtungen führen, sollten nach Möglichkeit unterirdisch verlegt oder mit einem angemessenen alternativen Schutz versehen werden, z. B. durch einen Bodenkabelschutz und einen Strommast; sind die Kabel unterirdisch verlegt, sollten sie vor versehentlichem Durchtrennen geschützt werden (z. B. durch Panzerrohre oder Anwesenheitssignale);
- b) Separierung der Stromleitungen von den Telekommunikationsleitungen, 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 und Alarmen an Untersuchungs- und Endpunkten;
 - 2) Verwendung elektromagnetischer Abschirmung zum Schutz der Kabel;
 - 3) regelmäßige technische Sweeps und physische Untersuchungen zur Identifizierung unberechtigter Geräte, die an die Kabel angeschlossen werden;
 - 4) kontrollierter Zugang zu Schalttafeln und Kabelräumen (z. B. mit mechanischen Schlüsseln oder PINs);
 - 5) Verwendung von Glasfaserkabeln;
- d) Kennzeichnung der Kabel an jedem Ende mit ausreichenden Angaben zur Quelle und zum Ziel, um die physische Identifizierung und Überprüfung des Kabels zu ermöglichen.

Es sollte fachlicher Rat eingeholt werden, wie mit Risiken umzugehen ist, die sich aus Vorfällen oder Fehlfunktionen in der Verkabelung ergeben.

Weitere Informationen

Manchmal sind Strom- und Telekommunikationsverkabelung gemeinsame Ressourcen für mehr als eine Organisation, die an einem gemeinsamen Standort untergebracht sind.

7.13 Instandhaltung von Geräten und Betriebsmitteln

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz #Resilienz

Maßnahme

Geräte und Betriebsmittel sollten ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.

Zweck

Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Gefährdung von Informationen und anderen zugehörigen Werten oder der Unterbrechung der Betriebsabläufe der Organisation aufgrund mangelnder Wartung.

Leitfaden

Die folgenden Richtlinien zur Wartung von Geräten und Betriebsmitteln sollten dabei berücksichtigt werden:

- a) Wartung der Geräte und Betriebsmittel entsprechend den empfohlenen Serviceintervallen und Spezifikationen des Lieferanten;
- b) Umsetzung und Überwachung eines Instandhaltungsprogramms durch die Organisation;

- c) Durchführung von Reparaturen und Wartungsarbeiten an Geräten ausschließlich von befugten Beschäftigten;
- d) Dokumentation aller vermuteten und tatsächlichen Fehler sowie aller vorbeugenden und Korrekturmaßnahmen;
- e) Umsetzung geeigneter Maßnahmen, wenn Geräte und Betriebsmittel zur Wartung vorgesehen sind, unter Berücksichtigung der Tatsache, ob diese Wartung von Beschäftigten vor Ort oder von Externen durchgeführt wird. Verpflichtung des Wartungspersonals zu einer geeigneten Vertraulichkeitsvereinbarung;
- f) Überwachung des Wartungspersonals bei der Durchführung von Wartungsarbeiten vor Ort;
- g) Autorisierung und Kontrolle des Zugangs für die Fernwartung;
- h) Anwendung von Sicherheitsmaßnahmen für Werte außerhalb des Betriebsgeländes (siehe 7.9), wenn Geräte, die Informationen enthalten, zu Wartungszwecken außer Haus gebracht werden;
- i) Einhaltung aller von der Versicherung auferlegten Wartungsanforderungen;
- j) vor der Wiederinbetriebnahme von Geräten und Betriebsmitteln nach der Wartung deren Untersuchung, um sicherzustellen, dass sie nicht manipuliert wurden und einwandfrei funktionieren;
- k) Anwendung von Maßnahmen zur sicheren Entsorgung oder Wiederverwendung von Geräten (siehe 7.14), wenn festgelegt ist, dass die Geräte entsorgt werden sollen.

Weitere Informationen

Zu den Geräten gehören technische Komponenten von Informationsverarbeitungsanlagen, unterbrechungs-freie Stromversorgungen (USV) und Batterien, Stromgeneratoren, Wechselstromgeneratoren und -wandler, physische Einbruchmeldeanlagen und Alarmer, Rauchmelder, Feuerlöscher, Klimaanlage und Aufzüge.

7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Maßnahmenart	Informationssicher- heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz

Maßnahme

Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, sollten überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.

Zweck

Verhinderung, dass Informationen aus Geräten, die entsorgt oder wiederverwendet werden sollen, nach außen dringen.

Leitfaden

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

Speichermedien, die vertrauliche oder urheberrechtlich geschützte Informationen enthalten, sollten anstelle der Anwendung der standardmäßigen Löschfunktion physisch zerstört oder die Informationen sollten mittels geeigneter Verfahren dergestalt zerstört, gelöscht oder überschrieben werden, dass die ursprünglichen Informationen nicht wiederhergestellt werden können. Eine ausführliche Anleitung zur sicheren Entsorgung von Speichermedien ist unter 7.10 zu finden, Anleitung zur Löschung von Informationen unter 8.10.

Etiketten und Kennzeichnung, die die Organisation identifizieren oder die Klassifizierung, den Eigentümer, das System oder das Netzwerk angeben, sollten vor der Entsorgung, einschließlich des Weiterverkaufs oder der Spende an eine Wohltätigkeitsorganisation, entfernt werden.

Die Organisation sollte die Entfernung von Sicherheitsmaßnahmen wie Zutrittskontrollen oder Überwachungseinrichtungen bei Beendigung des Mietverhältnisses oder beim Auszug aus den Räumlichkeiten in Betracht ziehen. Dies hängt u. a. von folgenden Faktoren ab:

- a) ihrem Mietvertrag, um den ursprünglichen Zustand der Einrichtung wiederherzustellen;
- b) Minimierung des Risikos, dass Systeme mit sensiblen Informationen dem nächsten Mieter überlassen werden (z. B. Benutzerzugangslisten, Video- oder Bilddateien);
- c) die Möglichkeit, die Maßnahmen in der nächsten Einrichtung wieder zu verwenden.

Weitere Informationen

Beschädigte Geräte und Betriebsmittel, die Datenträger beinhalten, können eine Risikoeinschätzung erfordern, 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 Geräten und Betriebsmitteln unter folgenden Voraussetzungen verringern:

- a) das Verschlüsselungsverfahren ist stark genug und umfasst tatsächlich den gesamten Datenträger (einschließlich Schlupfspeicher, Ausgliederungsdateien);
- b) die kryptographischen Schlüssel sind lang genug, um Brute-Force-Angriffen standzuhalten;
- c) die kryptographischen Schlüssel werden ihrerseits sicher aufbewahrt (und z. B. auf keinen Fall auf demselben Datenträger gespeichert).

Weitere Empfehlungen zur Kryptographie sind unter 8.24 zu finden.

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

Siehe ISO/IEC 27040 für Einzelheiten über Verfahren zur Löschung von Speichermedien.

8 Technologische Maßnahmen

8.1 Endpunktgeräte des Benutzers

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Schutz

Maßnahme

Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, sollten geschützt werden.

Zweck

Schutz von Informationen vor den Risiken, die durch die Verwendung von Benutzerendpunktgeräten entstehen.

Leitfaden

Allgemeines

Die Organisation sollte eine themenspezifische Richtlinie zur sicheren Konfiguration und Handhabung von Benutzerendpunktgeräten erstellen. Die themenspezifische Richtlinie sollte allen zuständigen Mitarbeitern mitgeteilt werden und folgende Punkte berücksichtigen:

- die Art der Informationen und die Klassifizierungsstufe, die die Endpunktgeräte des Benutzers handhaben, verarbeiten, speichern oder unterstützen können;
- Registrierung der Benutzerendpunktgeräte;
- Anforderungen für den physischen Schutz;
- Einschränkung der Software-Installation (z. B. durch Systemadministratoren ferngesteuert);
- Anforderungen an die Software von Benutzerendpunktgeräten (einschließlich Softwareversionen) und an die Anwendung von Updates (z. B. aktive automatische Aktualisierung);
- Regeln für die Verbindung zu Informationsdiensten, öffentlichen Netzen oder anderen Netzen außerhalb des Gebäudes (z. B. die Verwendung einer persönlichen Firewall);
- Zugangssteuerungen;
- Verschlüsselung von Speichergeräten;
- Schutz gegen Schadsoftware;
- Remote-Deaktivierung, Löschung oder Sperrung;
- Datensicherungen;

- l) Nutzung von Web-Diensten und Web-Anwendungen;
- m) Analyse des Endnutzerverhaltens (siehe 8.16);
- n) die Verwendung von Wechseldatenträgern, einschließlich Wechselspeichergeräten, und die Möglichkeit, physische Anschlüsse (z. B. USB-Anschlüsse) zu deaktivieren;
- o) die Verwendung von Partitionierungsfunktionen, sofern diese vom Endpunktgerät des Benutzers unterstützt werden, mit denen die Informationen der Organisation und andere zugehörige Werte (z. B. Software) sicher von anderen Informationen und anderen zugehörigen Werten auf dem Gerät getrennt werden können.

Es sollte überlegt werden, ob bestimmte Informationen so sensibel sind, dass sie nur über die Endpunktgeräte der Benutzer abgerufen werden können, aber nicht auf diesen Geräten gespeichert werden dürfen. In solchen Fällen können zusätzliche technische Sicherheitsvorkehrungen am Gerät erforderlich sein. So sollte z. B. sichergestellt werden, dass das Herunterladen von Dateien für die Offline-Arbeit deaktiviert ist und dass der lokale Speicher, z. B. die SD-Karte, deaktiviert ist.

Die Empfehlungen zu dieser Maßnahme sollten so weit wie möglich durch Konfigurationsmanagement (siehe 8.9) oder automatisierte Werkzeuge durchgesetzt werden.

Benutzerverantwortlichkeit

Allen Benutzern sollten die Sicherheitsanforderungen und -verfahren zum Schutz der Benutzerendpunktgeräte sowie über ihre Verantwortlichkeiten bei der Umsetzung dieser Sicherheitsmaßnahmen bekannt sein. Die Benutzer sollten angewiesen werden, die folgenden Grundsätze zu beachten:

- a) Abmeldung von aktiven Sitzungen und Beendigung von nicht mehr benötigten Diensten;
- b) Schutz der Benutzerendpunktgeräte vor unbefugter Nutzung durch eine physische Maßnahme (z. B. Schlüsselsperre oder spezielle Schlösser) und eine logische Maßnahme (z. B. Kennwortzugang), wenn sie nicht in Gebrauch sind; keine Geräte mit wichtigen, sensiblen oder kritischen Geschäftsinformationen unbeaufsichtigt lassen;
- c) die Geräte sind an öffentlichen Orten, in Großraumbüros, an Versammlungsorten und in anderen ungeschützten Bereichen mit besonderer Vorsicht zu verwenden (z. B. dürfen vertrauliche Informationen nicht gelesen werden, wenn andere Personen sie von hinten lesen können, und es sind Sichtschutzfilter zu verwenden);
- d) physischer Schutz der Endpunktgeräte der Benutzer vor Diebstahl (z. B. in Autos und anderen Verkehrsmitteln, Hotelzimmern, Konferenzzentren und Versammlungsorten).

Für den Fall des Diebstahls oder Verlusts von Benutzerendpunktgeräten sollte ein spezielles Verfahren unter Berücksichtigung rechtlicher, gesetzlicher, regulatorischer, vertraglicher (einschließlich versicherungstechnischer) und anderer Sicherheitsanforderungen entwickelt werden.

Verwendung persönlicher Geräte

Wenn die Organisation die Verwendung persönlicher Geräte (manchmal auch als BYOD bezeichnet) zulässt, sollten zusätzlich zu den in dieser Maßnahme gegebenen Leitlinien die folgenden Punkte berücksichtigt werden:

- a) Trennung von persönlicher und geschäftlicher Nutzung der Geräte, einschließlich Software zur Unterstützung dieser Trennung und zum Schutz von geschäftlichen Daten auf privaten Geräten;

- b) Zugriff auf geschäftliche Daten erst, nachdem Benutzer ihre Pflichten anerkannt haben (physischer Schutz, Software-Aktualisierung usw.), ihren Verzicht auf das Eigentum von Geschäftsdaten erklären und der Organisation im Fall des Diebstahls oder Verlusts des Gerätes oder bei Wegfall der Befugnis zur Dienstbenutzung das Löschen der Daten per Fernzugriff zu erlauben. In solchen Fällen sollten Rechtsvorschriften zum Schutz personenbezogener Daten in Betracht gezogen werden;
- c) themenspezifische Richtlinien und Verfahren, um Streitigkeiten über Rechte an geistigem Eigentum zu verhindern, das auf privaten Geräten erarbeitet wurde;
- d) Zugang zu Geräten in Privateigentum (um die Sicherheit der Maschine zu überprüfen oder während einer Untersuchung), der von Gesetzes wegen verhindert werden kann;
- e) Software-Lizenzvereinbarungen, die dergestalt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Benutzerendpunktgeräten von Mitarbeitern oder sonstiger Benutzer, die zu externen Parteien gehören, verantwortlich werden können.

Drahtlose Verbindungen

Die Organisation sollte Verfahren einrichten für:

- a) die Konfiguration von drahtlosen Verbindungen auf Geräten (z. B. Deaktivierung anfälliger Protokolle);
- b) die Nutzung von drahtlosen oder kabelgebundenen Verbindungen mit angemessener Bandbreite in Übereinstimmung mit den einschlägigen themenspezifischen Richtlinien (z. B. weil Backups oder Software-Updates erforderlich sind).

Weitere Informationen

Die Maßnahmen zum Schutz von Informationen auf Benutzerendpunktgeräten hängen davon ab, ob das Benutzerendpunktgerät nur innerhalb der gesicherten Räumlichkeiten und Netzwerkverbindungen der Organisation verwendet wird, oder ob es außerhalb der Organisation erhöhten physischen und netzwerkbezogenen Bedrohungen ausgesetzt ist.

Die drahtlosen Verbindungen für Benutzerendpunktgeräte sind anderen Arten von Netzwerkverbindungen ähnlich, zeigen allerdings wesentliche Unterschiede, die bei der Ermittlung von Maßnahmen berücksichtigt werden sollten. Insbesondere die Sicherung von Informationen, die auf den Endpunktgeräten der Benutzer gespeichert sind, kann manchmal aufgrund der begrenzten Netzwerkbandbreite fehlschlagen oder weil die Endpunktgeräte der Benutzer zum Zeitpunkt der geplanten Sicherung nicht verbunden sind.

Bei einigen USB-Anschlüssen, wie z. B. USB-C, ist die Deaktivierung des USB-Anschlusses nicht möglich, da er für andere Zwecke verwendet wird (z. B. für die Stromversorgung und die Bildschirmausgabe).

8.2 Privilegierte Zugangsrechte

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Zuteilung und Gebrauch von privilegierten Zugangsrechten sollte eingeschränkt und verwaltet werden.

Zweck

Es wird sichergestellt, dass nur autorisierte Benutzer, Softwarekomponenten und Dienste mit privilegierten Zugangsrechten ausgestattet werden.

Leitfaden

Die Zuteilung von privilegierten Zugangsrechten sollte durch einen Genehmigungsprozess entsprechend der jeweiligen themenspezifischen Richtlinie zur Zugangssteuerung (siehe 5.15) kontrolliert werden. Folgendes sollte berücksichtigt werden:

- a) Ermittlung der Benutzer, die für jedes System oder jeden Prozess (z. B. Betriebssysteme, Datenbankverwaltungssysteme und Anwendungen) privilegierte Zugangsrechte benötigen;
- b) Zuteilung von privilegierten Zugangsrechten an Benutzer je nach Bedarf und Ereignis im Einklang mit der themenspezifischen Richtlinie zur Zugangssteuerung (siehe 5.15) (d. h. nur an Personen mit der erforderlichen Kompetenz zur Durchführung von Tätigkeiten, die einen privilegierten Zugang erfordern, und auf der Grundlage der Mindestanforderungen für ihre funktionalen Rollen);
- c) Aufrechterhaltung eines Autorisierungsprozesses (d. h. Festlegung, wer privilegierte Zugangsrechte genehmigen kann, oder Nichtgewährung privilegierter Zugangsrechte, bis der Autorisierungsprozess abgeschlossen ist) und Aufzeichnung aller zugewiesenen Privilegien;
- d) Festlegung und Umsetzung der Anforderungen bezüglich des Auslaufens von privilegierten Zugangsrechten;
- e) Ergreifen von Maßnahmen, um sicherzustellen, dass die Benutzer ihre privilegierten Zugangsrechte kennen und wissen, wann sie sich im privilegierten Zugangsmodus befinden. Mögliche Maßnahmen sind die Verwendung bestimmter Benutzerkennungen, Einstellungen der Benutzeroberfläche oder sogar bestimmter Geräte;
- f) die Authentifizierungsanforderungen für privilegierte Zugangsrechte können höher sein als die Anforderungen für normale Zugangsrechte. Eine erneute Authentifizierung oder eine Authentifizierungsstufe kann erforderlich sein, bevor Arbeiten mit privilegierten Zugangsrechten durchgeführt werden;
- g) regelmäßige Überprüfung der Benutzer, die mit privilegierten Zugangsrechten arbeiten, nach jeder organisatorischen Änderung, um festzustellen, ob ihre Aufgaben, Rollen, Verantwortlichkeiten und Kompetenzen sie noch für die Arbeit mit privilegierten Zugangsrechten qualifizieren (siehe 5.18);
- h) Festlegung spezifischer Regeln, um die Nutzung von Benutzerkennungen mit allgemeinen Administratorrechten (z. B. „Stamm“) zu vermeiden, je nach den Konfigurationsmöglichkeiten der Systeme. Verwaltung und Schutz der Authentifizierungsinformationen solcher Identitäten (siehe 5.17);
- i) Gewährung eines zeitlich begrenzten privilegierten Zugangs nur für den Zeitraum, der für die Umsetzung genehmigter Änderungen oder Aktivitäten erforderlich ist (z. B. für Wartungstätigkeiten oder einige kritische Änderungen), anstelle einer dauerhaften Gewährung privilegierter Zugangsrechte. Dies wird oft als „Break-Glass“-Verfahren bezeichnet und häufig durch Technologien zur Verwaltung von Zugangsrechten automatisiert;
- j) Protokollierung aller privilegierten Zugänge auf Systeme zu Prüfzwecken;

- k) keine gemeinsame Nutzung oder Verknüpfung von Identitäten mit privilegierten Zugangsrechten für mehrere Personen, sondern Zuweisung einer eigenen Identität für jede Person, die die Zuweisung spezifischer privilegierter Zugangsrechte ermöglicht. Identitäten können gruppiert werden (z. B. durch Definition einer Administratorgruppe), um die Verwaltung von privilegierten Zugangsrechten zu vereinfachen;
- l) Verwendung von Identitäten mit privilegierten Zugangsrechten nur für die Durchführung von Verwaltungsaufgaben und nicht für alltägliche allgemeine Aufgaben [d. h. Abrufen von E-Mails, Zugriff auf das Internet (die Benutzer sollten für diese Tätigkeiten eine separate normale Netzwerkidentität haben)].

Weitere Informationen

Privilegierte Zugangsrechte sind Zugangsrechte, die einer Identität, einer Rolle oder einem Prozess gewährt werden und die die Durchführung von Aktivitäten ermöglichen, die normale Benutzer oder Prozesse nicht durchführen können. Systemadministratorenrollen erfordern in der Regel privilegierte Zugangsrechte.

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

Weitere Informationen zur Zugangsverwaltung und zur sicheren Verwaltung des Zugangs zu Informationen und Ressourcen der Informations- und Kommunikationstechnologie finden sich in ISO/IEC 29146.

8.3 Informationszugangsbeschränkung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Der Zugang zu Informationen und anderen zugehörigen Werten sollte in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.

Zweck

Sicherstellung, dass nur befugte Benutzer Zugang haben und unbefugter Zugang auf Informationen und andere zugehörige Werte unterbunden wird.

Leitfaden

Der Zugang zu Informationen und anderen zugehörigen Werten sollte in Übereinstimmung mit den festgelegten themenspezifischen Richtlinien eingeschränkt werden. Die folgenden Punkte sollten zur Unterstützung der Zugangsbeschränkungsanforderungen berücksichtigt werden:

- a) keinen Zugang zu sensiblen Informationen durch unbekannte Benutzeridentitäten oder anonym zu ermöglichen. Öffentlicher oder anonymer Zugang sollte nur zu Speicherorten gewährt werden, die keine sensiblen Informationen enthalten;

- b) Bereitstellung von Konfigurationsmechanismen für die Steuerung des Zugangs zu Informationen in Systemen, Anwendungen und Diensten;
- c) Steuerung auf welche Daten ein einzelner Benutzer Zugang hat;
- d) Steuerung, welche Identitäten oder Gruppen von Identitäten welchen Zugang haben, z. B. Lesen, Schreiben, Löschen und Ausführen;
- e) Bereitstellung physischer oder logischer Zugangssteuerungen zur Isolierung sensibler Anwendungen, Anwendungsdaten oder Systeme.

Darüber hinaus sollten dynamische Zugangsverwaltungstechniken und -prozesse zum Schutz sensibler Informationen, die einen hohen Wert für die Organisation haben, in Betracht gezogen werden, wenn die Organisation:

- a) eine genaue Steuerung benötigt, wer in welchem Zeitraum und auf welche Weise auf diese Informationen zugreifen kann;
- b) solche Informationen mit Personen außerhalb der Organisation teilen und die Kontrolle darüber behalten möchte, wer darauf zugreifen kann;
- c) die Nutzung und Verbreitung dieser Informationen dynamisch und in Echtzeit verwalten möchte;
- d) diese Informationen gegen unbefugte Änderungen, Vervielfältigung und Verbreitung (einschließlich Druck) schützen möchte;
- e) die Nutzung der Informationen überwachen möchte;
- f) alle Änderungen an diesen Informationen aufzeichnen möchte, falls eine künftige Untersuchung erforderlich ist.

Dynamische Zugangsverwaltungstechniken sollten Informationen im Verlauf ihres Lebenszyklus evaluieren (d. h. Erstellung, Verarbeitung, Speicherung, Übertragung und Entsorgung) schützen, einschließlich:

- a) Festlegung von Regeln für die Verwaltung des dynamischen Zugangs auf der Grundlage spezifischer Anwendungsfälle unter Berücksichtigung:
 - 1) Gewährung von Zugangsberechtigungen auf der Grundlage von Identität, Gerät, Standort oder Anwendung;
 - 2) Nutzung des Klassifizierungsschemas, um festzustellen, welche Informationen durch dynamische Zugangsverwaltungstechniken geschützt werden müssen;
- b) Einrichtung von Betriebs-, Überwachungs- und Berichterstattungsverfahren sowie einer unterstützenden technischen Infrastruktur.

Dynamische Zugangsverwaltungssysteme sollten Informationen schützen, indem sie:

- a) eine Authentifizierung, entsprechende Anmeldedaten oder ein Zertifikat für den Zugriff auf Informationen erfordern;
- b) den Zugang, z. B. auf einen bestimmten Zeitraum (z. B. nach einem bestimmten Datum oder bis zu einem bestimmten Datum), beschränken;
- c) eine Verschlüsselung zum Schutz von Informationen verwenden;

- d) die Druckberechtigungen für die Informationen festlegen;
- e) aufzeichnen, wer auf die Informationen zugreift und wie die Informationen verwendet werden;
- f) Warnungen auslösen, wenn Versuche, die Informationen zu missbrauchen, entdeckt werden.

Weitere Informationen

Dynamische Zugangsverwaltungstechniken und andere dynamische Informationsschutztechnologien können den Schutz von Informationen auch dann unterstützen, wenn Daten über die ursprüngliche Organisation hinaus weitergegeben werden, wo herkömmliche Zugangssteuerungen nicht durchgesetzt werden können. Sie können auf Dokumente, E-Mails oder andere Dateien mit Informationen angewandt werden, um den Zugriff auf den Inhalt zu beschränken und die Art und Weise des Zugriffs zu bestimmen. Es kann auf granularer Ebene erfolgen und im Laufe des Lebenszyklus der Informationen angepasst werden.

Dynamische Zugangsverwaltungstechniken ersetzen nicht die klassische Zugangsverwaltung [z. B. unter Verwendung von Zugriffsskontrolllisten (ACL)], sondern können weitere Faktoren für die Konditionalität, Echtzeitbewertung, Just-in-Time-Datenreduzierung und andere Verbesserungen hinzufügen, die für die sensibelsten Informationen nützlich sein können. Sie bieten eine Möglichkeit, den Zugang außerhalb der Organisationsumgebung zu steuern. Die Reaktion auf Vorfälle kann durch dynamische Zugangsverwaltungstechniken unterstützt werden, da die Berechtigungen jederzeit geändert oder widerrufen werden können.

Weitere Informationen über ein Rahmenwerk für die Zugangsverwaltung sind in ISO/IEC 29146 enthalten.

8.4 Zugriff auf den Quellcode

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung #Anwendungssicherheit #Sichere_Konfiguration	#Schutz

Maßnahme

Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken sollte angemessen verwaltet werden.

Zweck

Verhinderung der Einführung nicht genehmigter Funktionen, Vermeidung unbeabsichtigter oder böswilliger Änderungen und Wahrung der Vertraulichkeit von wertvollem geistigem Eigentum.

Leitfaden

Der Zugriff auf den Quellcode und zugehörige Elemente (wie Designs, Spezifikationen, Verifikations- und Validierungspläne) und Entwicklungswerkzeuge (z. B. Compiler, Builder, Integrationswerkzeuge, Prüfplattformen und -umgebungen) sollte streng kontrolliert werden.

Für den Quellcode kann dies durch die Steuerung der zentralen Speicherung dieses Codes, vorzugsweise in einem Quellcode-Verwaltungssystem, erreicht werden.

Der Lese- und Schreibzugriff auf den Quellcode kann je nach der Rolle des Mitarbeiters unterschiedlich sein. So kann beispielsweise der Lesezugriff auf den Quellcode innerhalb der Organisation allgemein gewährt werden, während der Schreibzugriff auf den Quellcode nur privilegierten Mitarbeitern oder bestimmten Eigentümern zur Verfügung steht. Wenn Code-Komponenten von mehreren Entwicklern innerhalb einer Organisation verwendet werden, sollte ein Lesezugriff auf ein zentrales Code-Repository eingerichtet werden. Wenn innerhalb einer Organisation Open-Source-Code oder Code-Komponenten von Drittanbietern verwendet werden, kann darüber hinaus Lesezugriff auf solche externen Code-Repositories in großem Umfang gewährt werden. Der Schreibzugriff sollte jedoch weiterhin eingeschränkt werden.

Die folgenden Richtlinien sollten beachtet werden, um den Zugang zu Software-Quellcode-Bibliotheken zu kontrollieren und die Gefahr einer Verfälschung der Computerprogramme zu verringern:

- a) Verwaltung des Software-Quellcodes und der Software-Quellcode-Bibliotheken nach festgelegten Verfahren;
- b) Gewährung von Lese- und Schreibzugriff auf den Quellcode auf der Grundlage der geschäftlichen Erfordernisse und unter Berücksichtigung des Risikos der Veränderung oder des Missbrauchs sowie nach festgelegten Verfahren;
- c) Aktualisierung des Quellcodes und der zugehörigen Elemente sowie die Gewährung des Zugriffs auf den Quellcode in Übereinstimmung mit den Änderungskontrollverfahren (siehe 8.32) und nur nach Erhalt einer entsprechenden Genehmigung;
- d) den Entwicklern keinen direkten Zugriff auf das Quellcode-Repository zu gewähren, sondern über Entwickler-Tools, die Aktivitäten und Berechtigungen für den Quellcode kontrollieren;
- e) Aufbewahrung von Programmlisten in einer sicheren Umgebung, in der der Lese- und Schreibzugriff angemessen verwaltet und zugewiesen werden sollte;
- f) Führung eines Audit-Protokolls über alle Zugriffe und Änderungen am Quellcode.

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.

Weitere Informationen

Wenn der Zugriff auf den Quellcode nicht ordnungsgemäß kontrolliert wird, kann der Quellcode verändert werden oder einige Daten in der Entwicklungsumgebung (z. B. Kopien von Produktionsdaten, Konfigurationsdetails) können von Unbefugten abgerufen werden.

8.5 Sichere Authentifizierung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz

Maßnahme

Sichere Authentifizierungstechnologien und -verfahren sollten auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.

Zweck

Sicherstellung, dass ein Benutzer oder eine Einrichtung sicher authentifiziert ist, wenn der Zugang zu Systemen, Anwendungen und Diensten gewährt wird.

Leitfaden

Es sollte ein geeignetes Authentifizierungsverfahren zur Bestätigung der Identität eines Benutzers, einer Software, von Nachrichten und anderen Entitäten gewählt werden.

Die Stärke einer Authentifizierung sollte der Klassifizierung der Daten angemessen sein, auf die zugegriffen werden soll. Sofern eine starke Authentifizierung und Identitätsverifizierung erforderlich ist, sollten Authentifizierungsalternativen zu Kennwörtern wie digitale Zertifikate, Smartcards, Token oder biometrische Verfahren verwendet werden.

Die Authentifizierungsinformationen sollten durch zusätzliche Authentifizierungsfaktoren für den Zugriff auf kritische Informationssysteme ergänzt werden (auch bekannt als Multi-Faktor-Authentifizierung). Die Verwendung einer Kombination aus mehreren Authentifizierungsfaktoren, z. B. was Sie wissen, was Sie haben und was Sie sind, verringert die Möglichkeiten für unbefugte Zugriffe. Die Multi-Faktor-Authentifizierung kann mit anderen Techniken kombiniert werden, um unter bestimmten Umständen zusätzliche Faktoren zu verlangen, die auf vordefinierten Regeln und Mustern beruhen, z. B. Zugang von einem ungewöhnlichen Ort, von einem ungewöhnlichen Gerät oder zu einer ungewöhnlichen Zeit.

Biometrische Authentifizierungsdaten sollten ungültig gemacht werden, wenn sie jemals kompromittiert werden. Die biometrische Authentifizierung kann je nach Einsatzbedingungen (z. B. Feuchte oder Alterung) nicht verfügbar sein. Um auf diese Probleme vorbereitet zu sein, sollte die biometrische Authentifizierung mit mindestens einem alternativen Authentifizierungsverfahren kombiniert werden.

Das Verfahren zur Anmeldung an einem System oder einer Anwendung sollte so gestaltet sein, dass das Risiko eines unbefugten Zugangs möglichst gering ist. Die Anmeldeverfahren und -technologien sollten unter Berücksichtigung der folgenden Punkte implementiert werden:

- a) keine Anzeige sensibler System- oder Anwendungsinformationen, bis der Anmeldevorgang erfolgreich abgeschlossen ist, um einem unbefugten Benutzer keine unnötige Hilfestellung zu geben;
- b) Anzeige einer allgemeinen Warnmeldung, dass nur befugte Benutzer Zugang zum System, zur Anwendung oder zum Dienst haben sollten;
- c) Verzicht auf Hilfmeldungen während des Anmeldevorgangs, die einem unbefugten Benutzer helfen würden (z. B. sollte das System bei Auftreten eines Fehlers nicht anzeigen, welcher Teil der eingegebenen Daten richtig oder falsch ist);
- d) Validierung der Anmeldedaten erst nach Eingabe aller Daten;
- e) Schutz vor Brute-Force-Anmeldeversuchen bei Benutzernamen und Kennwörtern [z. B. Verwendung eines vollständig automatisierten öffentlichen Turing-Tests zur Unterscheidung von Computern und Menschen (CAPTCHA), Zurücksetzen des Kennworts nach einer vordefinierten Anzahl von Fehlversuchen oder Sperren des Benutzers nach einer maximalen Anzahl von Fehlern];
- f) Protokollierung erfolgloser und erfolgreicher Anmeldeversuche;

- g) Auslösen eines Sicherheitsereignisses, wenn ein potentieller versuchter oder erfolgreicher Verstoß gegen die Anmeldekontrollen festgestellt wird (z. B. Senden einer Warnung an den Benutzer und die Systemadministratoren der Organisation, wenn eine bestimmte Anzahl falscher Kennwortversuche erreicht wurde);
- h) die Anzeige oder das Senden der folgenden Informationen auf einem separaten Kanal nach einer erfolgreichen Anmeldung:
 - 1) Datum und Uhrzeit der letzten erfolgreichen Anmeldung;
 - 2) Einzelheiten zu allen erfolglosen Anmeldeversuchen seit der letzten erfolgreichen Anmeldung;
- i) keine Anzeige des Kennworts im Klartext bei der Eingabe; in einigen Fällen kann es erforderlich sein, diese Funktion zu deaktivieren, um die Anmeldung des Benutzers zu erleichtern (z. B. aus Gründen der Zugänglichkeit oder um zu vermeiden, dass Benutzer wegen wiederholter Fehler gesperrt werden);
- j) keine Übertragung von Kennwörtern im Klartext über ein Netzwerk, um zu verhindern, dass sie von einem sogenannten „Sniffer“-Programm ausgespäht werden;
- k) Beendigung inaktiver Sitzungen nach einer vorgegebenen Zeitspanne, insbesondere an Hochrisiko-Standorten wie in öffentlichen oder externen Bereichen, die nicht dem Sicherheitsmanagement der Organisation unterstehen, oder auf Benutzerendpunktgeräten;
- l) Beschränkung der Verbindungszeiten bei Hochrisikoanwendungen, um zusätzliche Sicherheit und möglichst wenig Gelegenheit für unbefugte Zugangsversuche zu bieten.

Weitere Informationen

Zusätzliche Informationen über die Sicherheit der Entitätsauthentifizierung sind in ISO/IEC 29115 zu finden.

8.6 Kapazitätssteuerung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Integrität	#Identifizieren	#Aufrechterhaltung	#Governance_und_Ökosystem
#Detektiv	#Verfügbarkeit	#Schützen #Erkennen		#Schutz

Maßnahme

Die Nutzung von Ressourcen sollte überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.

Zweck

Sicherstellung der erforderlichen Kapazität der Informationsverarbeitungseinrichtungen, der Humanressourcen, der Büros und anderer Einrichtungen.

Leitfaden

Die Kapazitätsanforderungen für Informationsverarbeitungsanlagen, Personal, Büros und andere Einrichtungen sollten unter Berücksichtigung der Betriebswichtigkeit der betroffenen Systeme und Prozesse festgestellt werden.

Es sollte eine Abstimmung und Überwachung des Systems erfolgen, um die Verfügbarkeit der Systeme sicherzustellen und ggf. zu verbessern.

Die Organisation sollte Stresstests von Systemen und Diensten durchführen, um zu bestätigen, dass ausreichende Systemkapazitäten zur Verfügung stehen, um Spitzenleistungsanforderungen zu erfüllen.

Es sollten Maßnahmen 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 sollte Ressourcen mit langen Vorlaufzeiten bei der Bereitstellung oder hohen Kosten geschenkt werden. Daher sollten die Manager, Dienste- oder Produkteigentümer die Nutzung wichtiger Systemressourcen überwachen.

Die Manager sollten Kapazitätsinformationen nutzen, um potentielle Ressourcenbeschränkungen und Abhängigkeiten von Beschäftigten in Schlüsselpositionen festzustellen und zu vermeiden, die eine Bedrohung für die Systemsicherheit oder die Dienste darstellen können, und entsprechende Maßnahmen zu planen.

Die Bereitstellung einer ausreichenden Kapazität kann durch Steigerung der Kapazität oder Verringerung des Bedarfs erreicht werden. Um die Kapazität zu erhöhen, sollte Folgendes in Betracht gezogen werden:

- a) Einstellung von neuem Personal;
- b) die Beschaffung neuer Einrichtungen oder Räumlichkeiten;
- c) die Anschaffung leistungsfähigerer Verarbeitungssysteme, Arbeitsspeicher und Speicher;
- d) die Nutzung des Cloud Computing, dessen inhärente Merkmale direkt auf die Kapazitätsproblematik eingehen. Cloud Computing verfügt über Elastizität und Skalierbarkeit, die es ermöglichen, die für bestimmte Anwendungen und Dienste verfügbaren Ressourcen nach Bedarf schnell zu erweitern oder zu reduzieren.

Die folgenden Punkte sollten berücksichtigt werden, um die Nachfrage nach den Ressourcen der Organisation zu reduzieren:

- a) Löschung veralteter Daten (Speicherplatz);
- b) Entsorgung von Unterlagen in Papierform, deren Aufbewahrungsfrist abgelaufen ist (Freisetzung von Regalflächen);
- c) Außerbetriebnahme von Anwendungen, Systemen, Datenbanken oder Umgebungen;
- d) Optimierung von Batch-Prozessen und -Planung;
- e) Optimierung des Anwendungscodes oder von Datenbankabfragen;
- f) 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 Kapazitätssteuerungsplans in Betracht gezogen werden.

Weitere Informationen

Weitere Einzelheiten über die Elastizität und Skalierbarkeit von Cloud Computing sind in ISO/IEC TS 23167 zu finden.

8.7 Schutz gegen Schadsoftware

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz
#Detektiv	#Integrität	#Erkennen	#Informationsschutz	#Verteidigung
#Korrektiv	#Verfügbarkeit			

Maßnahme

Schutz gegen Schadsoftware sollte umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.

Zweck

Sicherstellung des Schutzes von Informationen und anderen damit verbundenen Werten gegen Schadsoftware.

Leitfaden

Der Schutz vor Schadsoftware sollte sich auf Schadsoftware-Erkennungs- und Reparatur-Software, eine Sensibilisierung für das Thema Informationssicherheit, geeignete Maßnahmen für den Systemzugriff und die Änderungssteuerung stützen. Der Einsatz von Schadsoftware-Erkennungs- und -Reparatursoftware allein ist in der Regel nicht ausreichend. Die folgenden Richtlinien sollten dabei berücksichtigt werden:

- Implementierung von Regeln und Maßnahmen, die die Verwendung nicht zugelassener Software verhindern oder aufdecken [z. B. Application Allowlisting (d. h. die Verwendung einer Liste mit zugelassenen Anwendungen)] (siehe 8.19 und 8.32);
- Umsetzung von Maßnahmen zur Verhinderung bzw. Erkennung der Nutzung bekannter oder potentieller Schadcode-Websites (z. B. Sperrliste);
- Behebung von Schwachstellen, die durch Schadsoftware ausgenutzt werden könnten [z. B. durch das Management technischer Schwachstellen (siehe 8.8 und 8.19)];
- Durchführung regelmäßiger automatischer Überprüfungen der Software und des Datenbestands von Systemen, insbesondere bei Systemen, die betriebswichtige Geschäftsprozesse unterstützen; Untersuchung vorhandener nicht genehmigter Dateien oder nicht genehmigter Änderungen;
- Erstellung von Schutzmaßnahmen gegen die Risiken, die mit der Beschaffung von Dateien und Software von oder über externe Netze oder auf einem anderen Medium verbunden sind;

- f) Installation und regelmäßige Aktualisierung von Software zur Erkennung und Reparatur von Schadsoftware, um Computer und elektronische Speichermedien zu scannen. Durchführung regelmäßiger Scans, die Folgendes umfassen:
 - 1) Untersuchung aller über Netzwerke empfangene oder über elektronische Speichermedien erhaltene Daten auf Schadsoftware vor der Verwendung;
 - 2) Scannen von E-Mail- und Instant-Messaging-Anhängen und Downloads vor der Verwendung auf Schadsoftware. Durchführung dieses Scans an verschiedenen Stellen (z. B. auf den E-Mail-Servern, auf den Desktop-Computern) und beim Zugang zum Netzwerk der Organisation;
 - 3) Scannen von Webseiten auf Schadsoftware beim Zugriff;
- g) Festlegung der Platzierung und Konfiguration von Tools zur Erkennung und Reparatur von Schadsoftware auf der Grundlage der Ergebnisse der Risikoeinschätzung und unter Berücksichtigung:
 - 1) von Grundsätzen für eine gründliche Verteidigung dort, wo sie am wirksamsten wären. Dies kann zum Beispiel zur Erkennung von Schadsoftware in einem Netzwerk-Gateway (in verschiedenen Anwendungsprotokollen wie E-Mail, Dateiübertragung und Web) sowie in Endpunktgeräten und Servern der Benutzer führen;
 - 2) von Ausweichtechniken der Angreifer (z.B. die Verwendung verschlüsselter Dateien) zur Verbreitung von Schadsoftware oder der Verwendung von Verschlüsselungsprotokollen zur Übertragung von Schadsoftware;
- h) es sollte sorgfältig darauf geachtet werden, dass es im Rahmen der Wartungs- und Notfallverfahren zu keiner Einschleusung von Schadsoftware kommt, die die normalen Maßnahmen gegen Schadsoftware umgehen können;
- i) Implementierung eines Verfahrens zur Genehmigung der vorübergehenden oder dauerhaften Deaktivierung einiger oder aller Maßnahmen gegen Schadsoftware, einschließlich Genehmigungsbehörden für Ausnahmen, dokumentierter Begründung und Überprüfungsdatum. Dies kann notwendig sein, wenn der Schutz vor Schadsoftware zu einer Unterbrechung des normalen Betriebs führt;
- j) Vorbereitung entsprechender Business-Continuity-Pläne zur Wiederherstellung nach Schadsoftware-Angriffen, einschließlich aller erforderlichen Daten und eines Software-Backups (einschließlich Online- und Offline-Backups) sowie Wiederherstellungsmaßnahmen (siehe 8.13);
- k) Isolierung von Umgebungen, in denen katastrophale Folgen auftreten können;
- l) Festlegung von Verfahren und Verantwortlichkeiten zum Umgang mit dem Schutz gegen Schadsoftware auf den Systemen, einschließlich zur Nutzungsschulung, zur Meldung über Schadsoftware-Angriffe und zu Wiederherstellungsmaßnahmen im Anschluss daran;
- m) Sensibilisierung oder Schulung (siehe 6.3) aller Benutzer, wie sie den Empfang, das Senden oder die Installation von mit Schadsoftware infizierten E-Mails, Dateien oder Programmen erkennen und möglicherweise eindämmen können [die unter n) und o) gesammelten Informationen können verwendet werden, um sicherzustellen, dass Sensibilisierung und Schulung auf dem neuesten Stand gehalten werden];
- n) Implementierung von Verfahren zur regelmäßigen Erhebung von Informationen über neue Schadsoftware, z. B. durch das Abonnieren von Mailinglisten oder die Überprüfung einschlägiger Websites;
- o) Verifizierung, dass Informationen über Schadsoftware, wie z. B. Warnmeldungen, aus qualifizierten und seriösen Quellen stammen (z. B. zuverlässige Internetseiten oder Anbieter von Software zur Erkennung von Schadsoftware) und korrekt und informativ sind.

Weitere Informationen

Auf einigen Systemen (z. B. einigen industriellen Steuerungssystemen) ist es nicht immer möglich, Software zu installieren, die vor Schadsoftware schützt. Einige Formen von Schadsoftware infizieren die Betriebssysteme und die Firmware von Computern so, dass herkömmliche Schadsoftwaremaßnahmen das System nicht säubern können und ein vollständiges Re-Imaging der Betriebssystemsoftware und manchmal auch der Firmware des Computers erforderlich ist, um einen sicheren Zustand wiederherzustellen.

8.8 Handhabung von technischen Schwachstellen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Bedrohungs- und Schwachstellenmanagement	#Governance_und_Ökosystem #Schutz #Verteidigung

Maßnahme

Es sollten Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.

Zweck

Die Ausnutzung technischer Schwachstellen wird verhindert.

Leitfaden

Identifizierung von technischen Schwachstellen

Die Organisation sollte als Voraussetzung für ein wirksames technisches Schwachstellenmanagement über ein genaues Inventar der Bestände (siehe 5.9 bis 5.14) verfügen; das Inventar sollte den Software-Anbieter, den Softwareramen, Versionsnummern, den aktuellen Verteilungsstand (z. B. die Angabe, welche Software auf welchen Systemen installiert ist) und die für die Software innerhalb der Organisation zuständige(n) Person(en) enthalten.

Um technische Schwachstellen zu ermitteln, sollte die Organisation Folgendes berücksichtigen:

- Festlegung und Einrichtung der Rollen und Zuständigkeiten im Zusammenhang mit dem technischen Schwachstellenmanagement, einschließlich der Überwachung auf Schwachstellen, der Risikobeurteilung von Schwachstellen, der Aktualisierung, Nachverfolgung von Werten und sämtlichen erforderlichen Koordinationsaufgaben;
- für Software und andere Technologien (auf der Grundlage des Bestandsverzeichnisses, siehe 5.9), Ermittlung von Informationsressourcen, die für die Ermittlung relevanter technischer Schwachstellen und die Aufrechterhaltung des Bewusstseins für diese Schwachstellen genutzt werden sollen. Aktualisierung der Liste der Informationsressourcen aufgrund von Änderungen im Inventar oder wenn andere neue oder nützliche Ressourcen gefunden werden;
- Verpflichtung der Lieferanten von Informationssystemen (einschließlich ihrer Komponenten), die Meldung, Behandlung und Offenlegung von Schwachstellen sicherzustellen, einschließlich der Anforderungen in den geltenden Verträgen (siehe 5.20);

- d) Einsatz von für die verwendeten Technologien geeigneten Schwachstellen-Scan-Tools zur Ermittlung von Schwachstellen und zur Überprüfung, ob die Schwachstellen erfolgreich gepatcht wurden;
- e) Durchführung von geplanten, dokumentierten und wiederholbaren Penetrationstests oder Vulnerabilitätsbewertungen durch kompetente und befugte Personen, um die Identifizierung von Schwachstellen zu unterstützen. Vorsicht ist geboten, da solche Aktivitäten zu einer Kompromittierung der Systemsicherheit führen können;
- f) Verfolgung der Verwendung von Bibliotheken und Quellcode von Drittanbietern auf Schwachstellen. Dies sollte in die sichere Codierung einbezogen werden (siehe 8.28).

Die Organisation sollte Verfahren und Fähigkeiten entwickeln, um:

- a) das Vorhandensein von Schwachstellen in ihren Produkten und Diensten, einschließlich aller darin verwendeten externen Komponenten, zu erkennen;
- b) Schwachstellenberichte aus internen oder externen Quellen zu erhalten.

Die Organisation sollte im Rahmen einer themenspezifischen Richtlinie zur Offenlegung von Schwachstellen eine öffentliche Kontaktstelle einrichten, damit Forscher und andere Personen in der Lage sind, Probleme zu melden. Die Organisation sollte Verfahren für die Meldung von Schwachstellen, Online-Meldeformulare und die Nutzung geeigneter Foren für den Austausch von Bedrohungsdaten oder Informationen einrichten. Die Organisation sollte auch Bonusprogramme in Betracht ziehen, bei denen Belohnungen als Anreiz angeboten werden, um Organisationen bei der Identifizierung von Schwachstellen zu unterstützen, damit diese entsprechend behoben werden können. Die Organisation sollte auch Informationen an die zuständigen Branchenverbände oder andere interessierte Parteien weitergeben.

Evaluierung von technischen Schwachstellen

Bei der Evaluierung festgestellter technischer Schwachstellen sollten die folgenden Leitlinien berücksichtigt werden:

- a) Analyse und Verifizierung von Berichten, um festzustellen, welche Reaktions- und Abhilfemaßnahmen erforderlich sind;
- b) Sobald eine potentielle technische Schwachstelle festgestellt wurde, werden die damit verbundenen Risiken und die zu ergreifenden Maßnahmen ermittelt. Solche Maßnahmen können die Aktualisierung anfälliger Systeme oder die Anwendung anderer Maßnahmen umfassen.

Ergreifen geeigneter Maßnahmen, um technische Schwachstellen zu beseitigen

Es sollte ein Managementprozess für die Software-Aktualisierung umgesetzt werden, um sicherzustellen, dass die aktuellsten genehmigten Patches und Anwendungsaktualisierungen für sämtliche berechnigte Software installiert werden. Falls Änderungen erforderlich sind, sollten die Originalsoftware aufbewahrt und die Änderungen an einer dafür bestimmten Kopie vorgenommen werden. 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.

Zur Behebung technischer Schwachstellen sollten die folgenden Leitlinien berücksichtigt werden:

- a) Ergreifen geeigneter und rechtzeitiger Maßnahmen als Reaktion auf die Feststellung potentieller technischer Schwachstellen; Festlegung eines Zeitplans für die Reaktion auf Meldungen über potentiell relevante technische Schwachstellen;

- b) je nach Dringlichkeit der Behebung einer technischen Schwachstelle Durchführung der Maßnahme nach den für die Änderungssteuerung geltenden Sicherheitsmaßnahmen (siehe 8.32) oder anhand der folgenden Abhilfemaßnahmen bei Informationssicherheitsvorfällen (siehe 5.26);
- c) ausschließliche Verwendung von Aktualisierungen aus legitimen Quellen (die intern oder extern sein können);
- d) Prüfen und Evaluieren von Aktualisierungen, bevor sie installiert werden, um sicherzustellen, dass sie wirksam sind und keine untragbaren Nebenwirkungen haben [d. h. wenn eine Aktualisierung verfügbar ist, Beurteilung der mit der Installation der Aktualisierung verbundenen Risiken (die von der Sicherheitslücke ausgehenden Risiken sollten mit dem Risiko der Installation der Aktualisierung verglichen werden)];
- e) vorrangige Behandlung von Systemen mit hohem Risiko;
- f) Entwicklung von Abhilfemaßnahmen (in der Regel Software-Updates oder Patches);
- g) Prüfung, um zu bestätigen, dass die Abhilfemaßnahmen wirksam sind;
- h) Bereitstellung von Mechanismen zur Verifizierung der Authentizität der Abhilfemaßnahmen;
- i) wenn kein Update verfügbar ist oder das Update nicht installiert werden kann, sind weitere Maßnahmen zu erwägen, wie z. B.:
 - 1) Anwendung von Abhilfemaßnahmen, die vom Softwarehersteller oder anderen einschlägigen Quellen vorgeschlagen werden;
 - 2) Abschaltung der Dienste bzw. Funktionen, die von der Schwachstelle betroffen sind;
 - 3) Anpassung bzw. Ergänzung der Zugriffssteuerung, z. B. Firewalls, an den Netzwerkgrenzen (siehe 8.20 bis 8.22);
 - 4) Abschirmung anfälliger Systeme, Geräte oder Anwendungen vor Angriffen durch den Einsatz geeigneter Verkehrsfilter (manchmal auch virtuelles Patching genannt);
 - 5) Verstärkung der Überwachung zur Erkennung stattfindender Angriffe;
 - 6) erhöhte Sensibilisierung für die Schwachstelle.

Wenn die Hersteller von erworbener Software regelmäßig Informationen über Sicherheitsaktualisierungen für ihre Software veröffentlichen und eine Möglichkeit zur automatischen Installation solcher Aktualisierungen anbieten, sollte die Organisation entscheiden, ob sie die automatische Aktualisierung nutzen will oder nicht.

Sonstige Überlegungen

Über alle Schritte des technischen Schwachstellenmanagements sollte ein Auditprotokoll geführt werden.

Der Prozess zur Handhabung technischer Schwachstellen sollte regelmäßig überwacht und bewertet werden, um seine Wirksamkeit und Effizienz sicherzustellen.

Ein wirkungsvoller Prozess zur Handhabung technischer Schwachstellen 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 auftretenden Sicherheitsvorfall entsprechend durchzuführende technische Verfahren zur Verfügung stehen.

Nutzt die Organisation einen Cloud-Dienst, der von einem Drittanbieter bereitgestellt wird, sollte das technische Schwachstellenmanagement der Ressourcen des Cloud-Diensteanbieters vom Cloud-Diensteanbieter sichergestellt werden. Die Verantwortlichkeiten des Cloud-Diensteanbieters für das technische Schwachstellenmanagement sollten Teil der Cloud-Dienstleistungsvereinbarung sein und Verfahren für die Meldung der Maßnahmen des Cloud-Diensteanbieters in Bezug auf technische Schwachstellen umfassen (siehe 5.23). Bei einigen Cloud-Diensten sind der Cloud-Diensteanbieter und der Cloud-Dienste-Kunde jeweils für bestimmte Aufgaben zuständig. So ist beispielsweise der Kunde eines Cloud-Dienstes für das Schwachstellenmanagement seiner eigenen, für die Cloud-Dienste genutzten Anlagen verantwortlich.

Weitere Informationen

Die Handhabung technischer Schwachstellen kann auch als Unterfunktion der Änderungssteuerung gesehen werden und dabei die Vorteile der Prozesse und Verfahren der Änderungssteuerung nutzen (siehe 8.32).

Es ist möglich, dass eine Aktualisierung das bestehende Problem nicht angemessen behebt und sogar zu negativen Nebeneffekten führt. Zudem ist nach der Anwendung einer Aktualisierung deren Deinstallation nicht ohne weiteres möglich.

Wenn eine angemessene Überprüfung der Aktualisierungen nicht möglich ist, z. B. aus Kostengründen oder aufgrund fehlender Ressourcen, kann über eine Zurückstellung der Aktualisierung 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.

Werden Software-Patches oder -Updates erstellt, kann das Unternehmen einen automatischen Aktualisierungsprozess in Betracht ziehen, bei dem diese Updates auf den betroffenen Systemen oder Produkten installiert werden, ohne dass der Kunde oder der Benutzer eingreifen muss. Wenn ein automatischer Aktualisierungsprozess angeboten wird, kann der Kunde oder Benutzer eine Option wählen, um die automatische Aktualisierung zu deaktivieren oder den Zeitpunkt der Installation der Aktualisierung zu steuern.

Wenn der Anbieter einen automatischen Aktualisierungsprozess anbietet und die Aktualisierungen auf den betroffenen Systemen oder Produkten installiert werden können, ohne dass ein Eingreifen erforderlich ist, entscheidet die Organisation, ob sie den automatischen Prozess anwendet oder nicht. Ein Grund, sich gegen eine automatische Aktualisierung zu entscheiden, besteht darin, die Kontrolle darüber zu behalten, wann die Aktualisierung durchgeführt wird. So kann beispielsweise eine Software, die für einen Geschäftsvorgang verwendet wird, erst dann aktualisiert werden, wenn der Vorgang abgeschlossen ist.

Eine Schwachstelle beim Scannen auf Schwachstellen ist die Tatsache, dass möglicherweise nicht alle Aspekte der Tiefenverteidigung berücksichtigt werden: Zwei Gegenmaßnahmen, die immer nacheinander eingesetzt werden, können Schwachstellen aufweisen, die durch die Stärken der jeweils anderen Maßnahme verdeckt werden. Die zusammengesetzte Gegenmaßnahme ist nicht anfällig, während ein Schwachstellenscanner melden kann, dass beide Komponenten anfällig sind. Die Organisation sollte daher bei der Überprüfung von Schwachstellenberichten und bei der Reaktion darauf sorgfältig vorgehen.

Viele Organisationen liefern Software, Systeme, Produkte und Dienstleistungen nicht nur innerhalb der Organisation, sondern auch an interessierte Parteien wie Kunden, Partner oder andere Nutzer. Diese Software, Systeme, Produkte und Dienstleistungen können Schwachstellen in der Informationssicherheit aufweisen, die die Sicherheit der Benutzer beeinträchtigen.

Organisationen können Abhilfemaßnahmen freigeben und Informationen über Schwachstellen an die Benutzer weitergeben (in der Regel durch einen öffentlichen Hinweis) und entsprechende Informationen für Software-Schwachstellen-Datenbankdienste bereitstellen.

Weitere Informationen über das Management technischer Schwachstellen bei der Nutzung von Cloud Computing finden Sie in der Normenreihe ISO/IEC 19086 und ISO/IEC 27017.

ISO/IEC 29147 enthält detaillierte Informationen über den Eingang von Berichten über Sicherheitslücken und die Veröffentlichung von Hinweisen auf Sicherheitslücken. ISO/IEC 30111 enthält detaillierte Informationen über den Umgang mit gemeldeten Schwachstellen und deren Behebung.

8.9 Konfigurationsmanagement

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration	#Schutz

Maßnahme

Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.

Zweck

Sicherstellen, dass Hardware, Software, Dienste und Netzwerke mit den erforderlichen Sicherheitseinstellungen korrekt funktionieren und die Konfiguration nicht durch unbefugte oder falsche Änderungen verändert wird.

Leitfaden

Allgemeines

Die Organisation sollte Prozesse und Werkzeuge definieren und implementieren, um die definierten Konfigurationen (einschließlich Sicherheitskonfigurationen) für Hardware, Software, Dienste (z. B. Cloud-Dienste) und Netzwerke sowohl für neu installierte Systeme als auch für betriebliche Systeme über deren gesamte Lebensdauer durchzusetzen.

Es sollten Rollen, Verantwortlichkeiten und Verfahren für die Handhabung existieren, um die zufriedenstellende Steuerung aller Konfigurationsänderungen sicherzustellen.

Standardvorlagen

Es sollten Standardvorlagen für die sichere Konfiguration von Hardware, Software, Diensten und Netzwerken festgelegt werden:

- Verwendung öffentlich zugänglicher Leitfäden (z. B. vordefinierte Vorlagen von Anbietern und unabhängigen Sicherheitsorganisationen);
- Berücksichtigung der erforderlichen Schutzstufe, um eine ausreichende Sicherheitsstufe zu bestimmen;
- Unterstützung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Normen und anderen Sicherheitsanforderungen;
- Prüfung der Durchführbarkeit und Anwendbarkeit von Sicherheitskonfigurationen im Kontext der Organisation.

Die Vorlagen sollten regelmäßig überprüft und aktualisiert werden, wenn neue Bedrohungen oder Schwachstellen behoben werden müssen oder wenn neue Software- oder Hardwareversionen eingeführt werden.

Bei der Erstellung von Standardvorlagen für die sichere Konfiguration von Hardware, Software, Diensten und Netzwerken sollten folgende Punkte berücksichtigt werden:

- a) Minimierung der Anzahl von Identitäten mit privilegierten oder administrativen Zugangsrechten;
- b) Deaktivierung unnötiger, ungenutzter oder unsicherer Identitäten;
- c) Deaktivierung oder Einschränkung von nicht benötigten Funktionen und Diensten;
- d) Beschränkung des Zugriffs auf leistungsstarke Dienstprogramme und Host-Parametereinstellungen;
- e) Synchronisierung der Uhren;
- f) Änderung der Standardauthentifizierungsdaten des Herstellers, wie z. B. Standardkennwörter, unmittelbar nach der Installation und Überprüfung anderer wichtiger sicherheitsrelevanter Standardparameter;
- g) Aufrufen von Timeout-Einrichtungen, die Computergeräte nach einer bestimmten Zeit der Inaktivität automatisch abmelden;
- h) Überprüfung, ob die Lizenzanforderungen erfüllt sind (siehe 5.32).

Verwaltung von Konfigurationen

Bestehende Konfigurationen von Hardware, Software, Diensten und Netzwerken sollten aufgezeichnet werden, und es sollte ein Protokoll über alle Konfigurationsänderungen geführt werden. Diese Aufzeichnungen sollten sicher gespeichert werden. Dies kann auf verschiedene Weise geschehen, z. B. durch Konfigurationsdatenbanken oder Konfigurationsvorlagen.

Änderungen an Konfigurationen sollten dem Änderungsmanagementprozess folgen (siehe 8.32).

Konfigurationsdatensätze können folgende Informationen enthalten:

- a) aktuelle Informationen über den Eigentümer oder die Kontaktstelle für den Wert;
- b) Datum der letzten Änderung der Konfiguration;
- c) Version der Konfigurationsvorlage;
- d) Verhältnis zu den Konfigurationen der anderen Werte.

Überwachung von Konfigurationen

Die Konfigurationen sollten mit einem umfassenden Satz von Systemmanagement-Tools (z. B. Wartungsprogramme, Fernsupport, Unternehmensmanagement-Tools, Sicherungs- und Wiederherstellungssoftware) überwacht und regelmäßig überprüft werden, um die Konfigurationseinstellungen zu verifizieren, die Kennwortstärke zu bewerten und die durchgeführten Aktivitäten zu beurteilen. Ist-Konfigurationen können mit den definierten Soll-Vorlagen verglichen werden. Auf Abweichungen sollte reagiert werden, entweder durch automatische Durchsetzung der definierten Sollkonfiguration oder durch manuelle Analyse der Abweichung und anschließende Korrekturmaßnahmen.

Weitere Informationen

In der Systemdokumentation werden häufig Einzelheiten über die Konfiguration von Hardware und Software festgehalten.

Die Systemhärtung ist ein typischer Teil des Konfigurationsmanagements.

Das Konfigurationsmanagement kann in die Prozesse der Anlagenverwaltung und die damit verbundenen Werkzeuge integriert werden.

Die Automatisierung ist in der Regel effektiver, um die Sicherheitskonfiguration zu verwalten (z. B. mit Infrastructure as Code).

Konfigurationsvorlagen und Ziele können vertrauliche Informationen sein und sollten entsprechend vor unbefugtem Zugriff geschützt werden.

8.10 Löschung von Informationen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Informationsschutz #Recht_und_Compliance	#Schutz

Maßnahme

Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.

Zweck

Verhinderung einer unnötigen Offenlegung sensibler Daten und Einhaltung gesetzlicher, satzungsmäßiger, behördlicher und vertraglicher Anforderungen an die Löschung von Daten.

Leitfaden

Allgemeines

Sensible Informationen sollten nicht länger als nötig aufbewahrt werden, um das Risiko einer unerwünschten Offenlegung zu verringern.

Beim Löschen von Informationen über Systeme, Anwendungen und Dienste sollte Folgendes beachtet werden:

- Auswahl eines Löschverfahrens (z. B. elektronisches Überschreiben oder kryptographische Löschung) in Übereinstimmung mit den Geschäftsanforderungen und unter Berücksichtigung der einschlägigen Gesetze und Vorschriften;
- die Aufzeichnung der Ergebnisse der Löschung als Beweismittel;
- bei der Inanspruchnahme von Dienstleistern für die Löschung von Informationen einen Nachweis über die Löschung von Informationen von ihnen zu erhalten.

Wenn Dritte die Daten der Organisation in ihrem Namen speichern, sollte die Organisation die Aufnahme von Anforderungen zur Löschung von Daten in die Vereinbarungen mit Dritten in Betracht ziehen, um diese während und nach Beendigung solcher Dienste durchzusetzen.

Löschungsverfahren

In Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Datenaufbewahrung und unter Berücksichtigung der einschlägigen Gesetze und Vorschriften sollten sensible Informationen gelöscht werden, wenn sie nicht mehr benötigt werden, durch:

- a) Konfiguration von Systemen zur sicheren Vernichtung von Informationen, wenn diese nicht mehr benötigt werden (z. B. nach einem bestimmten Zeitraum entsprechend der themenspezifischen Richtlinie zur Datenaufbewahrung oder auf Antrag der Betroffenen);
- b) Löschung veralteter Versionen, Kopien und temporärer Dateien, wo immer sie sich befinden;
- c) die Verwendung von zugelassener, sicherer Löschsoftware, um Informationen dauerhaft zu löschen und sicherzustellen, dass diese nicht durch spezielle Wiederherstellungs- oder forensische Tools wiederhergestellt werden können;
- d) über zugelassene, zertifizierte Anbieter von sicheren Entsorgungsdiensten;
- e) Verwendung von Entsorgungsmechanismen, die für die Art der zu entsorgenden Speichermedien geeignet sind (z. B. Entmagnetisierung von Festplattenlaufwerken und anderen magnetischen Speichermedien).

Bei der Nutzung von Cloud-Diensten sollte die Organisation prüfen, ob das vom Cloud-Anbieter angebotene Lösungsverfahren zulässig ist, und wenn dies der Fall ist, sollte die Organisation es nutzen oder den Cloud-Anbieter auffordern, die Informationen zu löschen. Diese Löschvorgänge sollten in Übereinstimmung mit den themenspezifischen Richtlinien automatisiert werden, sofern vorhanden und anwendbar. Je nach Sensibilität der gelöschten Informationen können Protokolle nachverfolgen oder nachweisen, dass diese Löschvorgänge stattgefunden haben.

Um zu vermeiden, dass sensible Informationen unbeabsichtigt preisgegeben werden, wenn die Geräte an die Lieferanten zurückgeschickt werden, sollten sensible Informationen geschützt werden, indem Zusatzspeicher (z. B. Festplatten) und Arbeitsspeicher entfernt werden, bevor die Geräte die Räumlichkeiten der Organisation verlassen.

In Anbetracht der Tatsache, dass die sichere Löschung einiger Geräte (z. B. Smartphones) nur durch Zerstörung oder durch die Nutzung der in diese Geräte integrierten Funktionen (z. B. „Wiederherstellen der Werkseinstellungen“) erreicht werden kann, sollte die Organisation das geeignete Verfahren je nach der Klassifizierung der von diesen Geräten verarbeiteten Informationen wählen.

Die in 7.14 beschriebenen Kontrollmaßnahmen sollten angewandt werden, um das Speichermedium physisch zu zerstören und gleichzeitig die darin enthaltenen Informationen zu löschen.

Ein offizielles Protokoll über die Löschung von Informationen ist nützlich bei der Analyse der Ursache eines möglichen Informationsverlusts.

Weitere Informationen

Informationen zur Löschung von Nutzerdaten in Cloud-Diensten finden sich in ISO/IEC 27017.

Informationen zur Löschung personenbezogener Daten sind in ISO/IEC 27555 zu finden.

8.11 Datenmaskierung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#Informationsschutz	#Schutz

Maßnahme

Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.

Zweck

Begrenzung der Offenlegung sensibler Daten, einschließlich personenbezogener Daten, und Einhaltung rechtlicher, gesetzlicher, regulatorischer und vertraglicher Anforderungen.

Leitfaden

Wenn der Schutz sensibler Daten (z. B. personenbezogene Daten) ein Anliegen ist, sollte die Organisation in Erwägung ziehen, solche Daten durch Techniken wie Datenmaskierung, Pseudonymisierung oder Anonymisierung zu verbergen.

Pseudonymisierungs- oder Anonymisierungstechniken können personenbezogene Daten verbergen, die wahre Identität des Auftraggebers der personenbezogenen Daten oder andere sensible Informationen verschleiern und die Verbindung zwischen personenbezogenen Daten und der Identität des Auftraggebers der personenbezogenen Daten oder die Verbindung zwischen anderen sensiblen Informationen aufheben.

Bei der Verwendung von Pseudonymisierungs- oder Anonymisierungstechniken sollte überprüft werden, ob die Daten angemessen pseudonymisiert oder anonymisiert wurden. Die Datenanonymisierung sollte alle Elemente der sensiblen Informationen berücksichtigen, um wirksam zu sein. So kann zum Beispiel eine Person, wenn sie nicht angemessen berücksichtigt wird, auch dann identifiziert werden, wenn die Daten, mit denen sie direkt identifiziert werden kann, durch das Vorhandensein weiterer Daten, mit denen die Person indirekt identifiziert werden kann, anonymisiert werden.

Weitere Techniken zur Datenmaskierung umfassen:

- a) Verschlüsselung (autorisierte Benutzer müssen einen Schlüssel haben);
- b) Nullen oder Löschen von Zeichen (um zu verhindern, dass nicht autorisierte Benutzer vollständige Nachrichten sehen können);
- c) unterschiedliche Zahlen und Daten;
- d) Substitution (Austausch eines Wertes gegen einen anderen, um sensible Daten zu verbergen);
- e) Ersetzen von Werten durch ihren Hash.

Bei der Implementierung von Datenmaskierungstechniken sollte Folgendes beachtet werden:

- a) nicht allen Benutzern Zugang zu allen Daten zu gewähren und daher Abfragen und Masken so zu gestalten, dass dem Nutzer nur die minimal erforderlichen Daten angezeigt werden;

- b) es gibt Fälle, in denen einige Daten aus einem Datensatz für den Benutzer nicht sichtbar sein sollten; in diesem Fall ist ein Mechanismus zur Verschleierung von Daten zu gestalten und zu implementieren (z. B. wenn ein Patient nicht möchte, dass das Krankenhauspersonal alle seine Daten sehen kann, selbst im Notfall, dann werden dem Krankenhauspersonal teilweise verschleierte Daten präsentiert, und der Zugriff auf die Daten ist nur für Personal mit bestimmten Rollen möglich, wenn sie nützliche Informationen für eine angemessene Behandlung enthalten);
- c) wenn Daten verschleiert werden, so dass die betroffene Person verlangen kann, dass die Benutzer nicht sehen können, ob die Daten verschleiert sind (Verschleierung der Verschleierung; dies wird z. B. in Gesundheitseinrichtungen verwendet, wenn der Patient nicht möchte, dass das Personal sieht, dass sensible Informationen wie Schwangerschaften oder Ergebnisse von Blutuntersuchungen verschleiert wurden);
- d) etwaige gesetzliche oder regulatorische Anforderungen (z. B. die Anforderung, die Daten von Zahlungskarten während der Verarbeitung oder Speicherung zu maskieren).

Bei der Verwendung von Datenmaskierung, Pseudonymisierung oder Anonymisierung sollte Folgendes beachtet werden:

- a) Stärke der Datenmaskierung, Pseudonymisierung oder Anonymisierung je nach der Verwendung der verarbeiteten Daten;
- b) Zugangssteuerungen zu den verarbeiteten Daten;
- c) Vereinbarungen oder Einschränkungen hinsichtlich der Verwendung der verarbeiteten Daten;
- d) das Verbot, die verarbeiteten Daten mit anderen Informationen abzugleichen, um die betroffene Person zu identifizieren;
- e) Verfolgung der Bereitstellung und des Eingangs der verarbeiteten Daten.

Weitere Informationen

Durch die Anonymisierung werden personenbezogene Daten unwiderruflich so verändert, dass die betroffene Person weder direkt noch indirekt identifiziert werden kann.

Bei der Pseudonymisierung werden die identifizierenden Informationen durch ein Pseudonym ersetzt. Die Kenntnis des Algorithmus (manchmal auch als „zusätzliche Informationen“ bezeichnet), der zur Durchführung der Pseudonymisierung verwendet wird, ermöglicht zumindest eine gewisse Form der Identifizierung der betroffenen Person. Solche „zusätzlichen Informationen“ sollten daher getrennt und geschützt aufbewahrt werden.

Obwohl die Pseudonymisierung also schwächer ist als die Anonymisierung, können pseudonymisierte Datensätze in der statistischen Forschung nützlicher sein.

Datenmaskierung ist eine Reihe von Techniken zum Verbergen, Ersetzen oder Verschleiern sensibler Datenelemente. Datenmaskierung kann statisch (wenn Datenelemente in der Originaldatenbank maskiert werden), dynamisch (unter Verwendung von Automatisierung und Regeln zur Sicherung von Daten in Echtzeit) oder on-the-fly (mit maskierten Daten im Speicher einer Anwendung) erfolgen.

Zur Anonymisierung von personenbezogenen Daten können Hash-Funktionen verwendet werden. Um Aufzählungsangriffe zu verhindern, sollten sie immer mit einer Salt-Funktion kombiniert werden.

Personenbezogene Daten in Ressourcenkennungen und ihren Attributen [z. B. Dateinamen, Uniform Resource Locators (URLs)] sollten entweder vermieden oder in geeigneter Weise anonymisiert werden.

Zusätzliche Maßnahmen zum Schutz personenbezogener Daten in öffentlichen Clouds sind in ISO/IEC 27018 enthalten.

Weitere Informationen zu De-Identifizierungsverfahren sind in ISO/IEC 20889 zu finden.

8.12 Verhinderung von Datenlecks

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv #Detektiv	#Vertraulichkeit	#Schützen #Erkennen	#Informationsschutz	#Schutz #Verteidigung

Maßnahme

Maßnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.

Zweck

Aufdeckung und Verhinderung der unbefugten Weitergabe und Extraktion von Informationen durch Personen oder Systeme.

Leitfaden

Die Organisation sollte Folgendes berücksichtigen, um das Risiko von Datenlecks zu verringern:

- Identifizierung und Klassifizierung von Informationen, um sie vor dem Verlust zu schützen (z. B. persönliche Informationen, Preismodelle und Produktdesigns);
- Überwachung der Kanäle, über die Daten nach außen dringen (z. B. E-Mail, Dateiübertragung, mobile Geräte und tragbare Speichergeräte);
- Maßnahmen, um zu verhindern, dass Informationen nach außen dringen (z. B. Quarantäne von E-Mails mit sensiblen Informationen).

Werkzeuge zur Verhinderung von Datenlecks sollten verwendet werden, um:

- sensible Informationen, bei denen die Gefahr einer unbefugten Offenlegung besteht (z. B. in unstrukturierten Daten auf dem System eines Benutzers) zu identifizieren und zu überwachen;
- die Offenlegung sensibler Informationen zu erkennen (z. B. wenn Informationen auf nicht vertrauenswürdige Cloud-Dienste Dritter hochgeladen oder per E-Mail versendet werden);
- Benutzeraktionen oder Netzübertragungen, die sensible Informationen preisgeben (z. B. Verhindern des Kopierens von Datenbankeinträgen in eine Tabellenkalkulation) zu blockieren.

Die Organisation sollte feststellen, ob es notwendig ist, die Fähigkeit eines Benutzers einzuschränken, Daten zu kopieren und einzufügen oder auf Dienste, Geräte und Speichermedien außerhalb der Organisation hochzuladen. Wenn dies der Fall ist, sollte das Unternehmen Technologien wie Tools zur Verhinderung von Datenlecks oder die Konfiguration vorhandener Tools implementieren, die es den Benutzern ermöglichen, Daten aus der Ferne einzusehen und zu bearbeiten, aber das Kopieren und Einfügen außerhalb der Kontrolle der Organisation verhindern.

Wenn ein Datenexport erforderlich ist, sollte der Dateneigentümer den Export genehmigen können und die Benutzer für ihre Handlungen zur Rechenschaft ziehen.

Das Anfertigen von Screenshots oder Fotografien des Bildschirms sollte in den Nutzungsbedingungen, in der Schulung und bei der Überprüfung berücksichtigt werden.

Bei der Sicherung von Daten sollte darauf geachtet werden, dass sensible Informationen durch Maßnahmen wie Verschlüsselung, Zugangssteuerung und physischen Schutz der Speichermedien, auf denen die Sicherung gespeichert ist, geschützt werden.

Die Verhinderung von Datenlecks sollte auch in Betracht gezogen werden, um einen Gegner davor zu schützen, vertrauliche oder geheime Informationen (geopolitischer, menschlicher, finanzieller, kommerzieller, wissenschaftlicher oder sonstiger Art) zu erlangen, die für Spionagezwecke von Interesse oder für die Gemeinschaft von entscheidender Bedeutung sein können. Die Maßnahmen zur Verhinderung von Datenlecks sollten darauf ausgerichtet sein, die Entscheidungen des Gegners zu verwirren, indem beispielsweise echte Informationen durch falsche Informationen ersetzt werden, entweder als eigenständige Maßnahme oder als Reaktion auf die nachrichtendienstlichen Maßnahmen des Gegners. Beispiele für diese Art von Aktionen sind Reverse Social Engineering oder die Verwendung von Honeypots, um Angreifer anzulocken.

Weitere Informationen

Tools zur Verhinderung von Datenlecks dienen der Identifizierung von Daten, der Überwachung der Datennutzung und -verschiebung sowie der Ergreifung von Maßnahmen, um Datenlecks zu verhindern (z. B. Warnung der Nutzer vor ihrem riskanten Verhalten und Blockierung der Datenübertragung auf tragbare Speichergeräte).

Die Verhinderung von Datenlecks beinhaltet zwangsläufig die Überwachung der Kommunikation und der Online-Aktivitäten der Mitarbeiter und damit auch der Nachrichten von Dritten, was rechtliche Bedenken aufwirft, die vor dem Einsatz von Tools zur Verhinderung von Datenlecks berücksichtigt werden sollten. Es gibt eine Vielzahl von Rechtsvorschriften in den Bereichen Privatsphäre, Datenschutz, Beschäftigung, Überwachung von Daten und Telekommunikation, die auf die Überwachung und Datenverarbeitung im Zusammenhang mit der Verhinderung von Datenlecks anwendbar sind.

Die Verhinderung von Datenlecks kann durch Standard-Sicherheitskontrollen unterstützt werden, z. B. durch themenspezifische Richtlinien zur Zugangssteuerung und zur sicheren Dokumentenverwaltung (siehe 5.12 und 5.15).

8.13 Sicherung von Information

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Korrektiv	#Integrität #Verfügbarkeit	#Wiederherstellen	#Aufrechterhaltung	#Schutz

Maßnahme

Sicherungskopien von Informationen, Software und Systemen sollten in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmäßig geprüft werden.

Zweck

Ermöglichung der Wiederherstellung nach einem Daten- oder Systemverlust.

Leitfaden

Es sollte eine themenspezifische Richtlinie zur Datensicherung erstellt werden, die den Anforderungen der Organisation an die Datenaufbewahrung und die Informationssicherheit gerecht wird.

Es sollten angemessene Datensicherungseinrichtungen vorhanden sein, um sicherzustellen, dass alle wichtigen Informationen und Softwareanwendungen nach einem Vorfall oder Versagen bzw. Verlust von Speichermedien wiederhergestellt werden können.

Es sollten Pläne entwickelt und umgesetzt werden, wie die Organisation Informationen, Software und Systeme sichern wird, um die themenspezifische Richtlinie zur Datensicherung zu erfüllen.

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

- a) Erstellung genauer und vollständiger Aufzeichnungen der Datensicherungskopien und der dokumentierten Wiederherstellungsverfahren;
- b) Widerspiegelung der geschäftlichen Anforderungen der Organisation (z. B. das Ziel des Wiederherstellungspunkts, siehe 5.30), der Sicherheitsanforderungen der betroffenen Informationen und der Bedeutung der Informationen für die Aufrechterhaltung des Betriebs der Organisation im Hinblick auf den Umfang (z. B. Voll- oder differenzielle Sicherung) und der Häufigkeit der Sicherungen;
- c) Aufbewahrung der Datensicherungen an einem externen Ort in ausreichender Entfernung, um vor Schäden am Hauptstandort geschützt zu sein;
- d) Gewährleistung eines angemessenen physischen und umweltbedingten Schutzes der Sicherungsinformationen (siehe Abschnitt 7 und 8.1), der den am Hauptstandort angewandten Normen entspricht;
- e) regelmäßige Prüfung der Sicherungsmedien, um sicherzustellen, dass sie im Notfall zuverlässig genutzt werden können. Prüfung der Fähigkeit, gesicherte Daten auf einem Prüfsystem wiederherzustellen, nicht durch Überschreiben der ursprünglichen Speichermedien, falls der Sicherungs- oder Wiederherstellungsprozess fehlschlägt und irreparable Datenschäden oder -verluste verursacht;
- f) Schutz der Datensicherungen durch Verschlüsselung entsprechend den ermittelten Risiken (z. B. in Situationen, in denen die Vertraulichkeit von Bedeutung ist);
- g) es ist darauf zu achten, dass ein versehentlicher Datenverlust erkannt wird, bevor die Sicherung durchgeführt wird.

Im Rahmen der Betriebsabläufe sollten die Durchführung von Datensicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Datensicherungen festgelegt werden, um die Vollständigkeit der Backups nach der themenspezifischen Richtlinie zu Datensicherungen sicherzustellen.

Datensicherungsmaßnahmen für einzelne Systeme und Dienste sollten regelmäßig überprüft werden, um sicherzustellen, dass sie die Ziele der Business ContinuityPläne erfüllen (siehe 5.30). Dies sollte mit einer Prüfung der Wiederherstellungsverfahren kombiniert und mit der im Plan zur Aufrechterhaltung der Betriebsfähigkeit vorgesehenen Wiederherstellungszeit verglichen werden. Bei betriebswichtigen Systemen und Diensten sollten die Datensicherungsmaßnahmen alle Systeminformationen, -anwendungen und -daten umfassen, die zur Wiederherstellung des kompletten Systems bei einem Schaden erforderlich sind.

Wenn die Organisation einen Cloud-Dienst nutzt, sollten Sicherungskopien der Informationen, Anwendungen und Systeme der Organisation in der Umgebung des Cloud-Dienstes erstellt werden. Die Organisation sollte bestimmen, ob und wie die Anforderungen an die Datensicherung erfüllt werden, wenn sie den als Teil des Cloud-Dienstes angebotenen Datensicherungsdienst nutzt.

Der Aufbewahrungszeitraum für wichtige geschäftliche Informationen sollte unter Berücksichtigung von Anforderungen zur Aufbewahrung von Archivkopien bestimmt werden. Die Organisation sollte die Löschung von Informationen (siehe 8.10) in Speichermedien, die für die Datensicherung verwendet werden, in Betracht ziehen, sobald die Aufbewahrungsfrist für die Informationen abgelaufen ist, und sollte dabei die Gesetze und Vorschriften berücksichtigen.

Weitere Informationen

Weitere Informationen zur Speichersicherheit, einschließlich Überlegungen zur Aufbewahrung, enthält die ISO/IEC 27040.

8.14 Redundanz von informationsverarbeitenden Einrichtungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Verfügbarkeit	#Schützen	#Aufrechterhaltung #Asset_Management	#Schutz #Resilienz

Maßnahme

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

Zweck

Der kontinuierliche Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.

Leitfaden

Die Organisation sollte die Anforderungen an die Verfügbarkeit von Geschäftsdienstleistungen und Informationssystemen feststellen. Die Organisation sollte eine Systemarchitektur mit angemessener Redundanz entwickeln und implementieren, um diese Anforderungen zu erfüllen.

Redundanz kann durch die teilweise oder vollständige Duplizierung von Informationsverarbeitungsanlagen erreicht werden (d. h. Ersatzkomponenten oder zwei von allem). Die Organisation sollte Verfahren für die Aktivierung der redundanten Komponenten und Verarbeitungseinrichtungen planen und umsetzen. In den Verfahren sollte festgelegt werden, ob die redundanten Komponenten und Verarbeitungstätigkeiten immer oder in Notfällen automatisch oder manuell aktiviert werden. Die redundanten Komponenten und Informationsverarbeitungseinrichtungen sollten die gleiche Sicherheitsstufe sicherstellen wie die primären Komponenten.

Es sollten Mechanismen vorhanden sein, die die Organisation bei einem Ausfall der Informationsverarbeitungsanlagen alarmieren, die Durchführung des geplanten Verfahrens ermöglichen und die weitere Verfügbarkeit während der Reparatur oder des Austauschs der Informationsverarbeitungsanlagen erlauben.

Die Organisation sollte Folgendes bei der Implementierung redundanter Systeme berücksichtigen:

- Abschluss von Verträgen mit zwei oder mehr Anbietern von Netzwerken und kritischen Informationsverarbeitungseinrichtungen, wie z. B. Internetdienstleistern;
- Verwendung redundanter Netze;
- Nutzung zweier geographisch getrennter Rechenzentren mit gespiegelten Systemen;

- d) Nutzung physisch redundanter Stromversorgungen oder -quellen;
- e) Nutzung mehrerer paralleler Instanzen von Softwarekomponenten mit automatischem Lastausgleich zwischen ihnen (zwischen Instanzen im selben Rechenzentrum oder in verschiedenen Rechenzentren);
- f) Vorhandensein doppelter Komponenten in Systemen (z. B. Prozessor, Festplatten, Speicher) oder in Netzen (z. B. Firewalls, Router, Switches).

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

Weitere Informationen

Es besteht ein enger Zusammenhang zwischen Redundanz und IKT-Bereitschaft für die Aufrechterhaltung der Business Continuity (siehe 5.30), insbesondere wenn kurze Wiederherstellungszeiten erforderlich sind. Viele der Redundanzmaßnahmen können Teil der IKT-Kontinuitätsstrategien und -lösungen sein.

Die Implementierung von Redundanzen kann Risiken für die Integrität (z. B. können Prozesse des Kopierens von Daten in duplizierte Komponenten zu Fehlern führen) oder die Vertraulichkeit (z. B. kann eine schwache Sicherheitsmaßnahme duplizierter Komponenten zu einer Kompromittierung führen) von Informationen und Informationssystemen mit sich bringen, die bei der Konzeption von Informationssystemen berücksichtigt werden müssen.

Die Redundanz in Informationsverarbeitungsanlagen ist in der Regel nicht auf die Nichtverfügbarkeit von Anwendungen aufgrund von Fehlern innerhalb einer Anwendung ausgerichtet.

Mit dem Einsatz von Public Cloud Computing ist es möglich, mehrere Live-Versionen von Informationsverarbeitungseinrichtungen an mehreren separaten physischen Standorten mit automatischem Ausfall und Lastausgleich zwischen ihnen zu haben.

Einige der Technologien und Techniken zur Bereitstellung von Redundanz und automatischer Ausfallsicherung im Zusammenhang mit Cloud-Diensten werden in ISO/IEC TS 23167 behandelt.

8.15 Protokollierung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen	#Handhabung_von_Informationssicherheitsereignissen	#Schutz #Verteidigung

Maßnahme

Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, sollten erstellt, gespeichert, geschützt und analysiert werden.

Zweck

Aufzeichnung von Ereignissen, Generierung von Beweisen, Sicherstellung der Integrität von Protokolldaten, Schutz vor unbefugtem Zugriff, Identifizierung von Informationssicherheitsereignissen, die zu einem Informationssicherheitsvorfall führen können, und Unterstützung von Untersuchungen.

Leitfaden

Allgemeines

Die Organisation sollte festlegen, zu welchem Zweck Protokolle erstellt werden, welche Daten gesammelt und protokolliert werden und welche protokollspezifischen Anforderungen zum Schutz und zur Handhabung der Protokolldaten bestehen. Dies sollte in einer themenspezifischen Richtlinie zur Protokollierung dokumentiert werden.

Die Ereignisprotokolle sollten für jedes Ereignis, soweit zutreffend, Folgendes enthalten:

- a) Benutzerkennungen;
- b) Systemaktivitäten;
- c) Datum, Uhrzeit und Einzelheiten relevanter Ereignisse (z. B. Anmeldung und Abmeldung);
- d) Geräteerkennung, Systemerkennung und Standort;
- e) Netzwerkadressen und Protokolle.

Die folgenden Ereignisse sollten für die Protokollierung berücksichtigt werden:

- a) erfolgreiche und abgelehnte Systemzugriffsversuche;
- b) erfolgreiche und abgelehnte Versuche, auf Daten oder andere Ressourcen zuzugreifen;
- c) Änderungen der Systemkonfiguration;
- d) Nutzung von Privilegien;
- e) Nutzung von Dienstprogrammen und Anwendungen;
- f) Dateien, auf die zugegriffen wurde, und die Art des Zugriffs, einschließlich des Löschens wichtiger Dateien;
- g) vom Zugriffskontrollsystem ausgelöste Alarmer;
- h) Aktivierung und Deaktivierung von Sicherheitssystemen wie des Schadsoftware- und des Angriffserkennungssystems;
- i) Erstellung, Änderung oder Löschung von Identitäten;
- j) Transaktionen, die von Benutzern in Anwendungen ausgeführt werden. In einigen Fällen handelt es sich bei den Anwendungen um einen Dienst oder ein Produkt, das von einem Dritten bereitgestellt oder betrieben wird.

Es ist wichtig, dass alle Systeme über synchronisierte Zeitquellen verfügen (siehe 8.17), da dies die Korrelation von Protokollen zwischen Systemen zur Analyse, Alarmierung und Untersuchung eines Vorfalls ermöglicht.

Schutz von Protokollen

Benutzer, auch solche mit privilegierten Zugangsrechten, sollten nicht die Erlaubnis haben, Protokolle über ihre eigenen Aktivitäten zu löschen oder zu deaktivieren. Sie können potentiell die Protokolle der Informationsverarbeitungsanlagen, die ihnen direkt unterstellt sind, manipulieren. Daher ist es notwendig, die Protokolle zu schützen und zu prüfen, um die Rechenschaftsfähigkeit für Benutzer mit privilegierten Zugangsrechten aufrecht zu erhalten.

Die Maßnahmen sollten auf den Schutz vor unbefugten 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) Nichtaufzeichnung von Ereignissen oder Überschreiben von bereits aufgezeichneten Ereignissen, wenn der Speicherplatz für eine Protokolldatei überschritten wird.

Zum Schutz der Protokolle sollten folgende Techniken in Betracht gezogen werden: kryptographisches Hashing, Aufzeichnung in einer Datei, die nur Anhänge enthält und nur gelesen werden kann, Aufzeichnung in einer öffentlichen Transparenzdatei.

Einige Audit-Protokolle können aufgrund von Anforderungen an die Datenaufbewahrung oder zum Sammeln von Beweismaterial (siehe 5.28) archiviert werden.

Wenn die Organisation System- oder Anwendungsprotokolle an einen Anbieter senden muss, um die Fehlersuche oder -behebung zu unterstützen, sollten die Protokolle vor der Übermittlung an den Anbieter nach Möglichkeit durch Datenmaskierungstechniken (siehe 8.11) von Informationen wie Benutzernamen, Internetprotokoll (IP)-Adressen, Hostnamen oder Organisationsnamen de-identifiziert werden.

Ereignisprotokolle können sensible Daten und personenbezogene Informationen enthalten. Daher sollten entsprechende Maßnahmen zum Schutz der Privatsphäre ergriffen werden (siehe 5.34).

Protokollanalyse

Die Protokollanalyse sollte die Analyse und Interpretation von Informationssicherheitsereignissen umfassen, um ungewöhnliche Aktivitäten oder anomales Verhalten zu erkennen, die auf eine Gefährdung hinweisen können.

Die Analyse von Ereignissen sollte unter Berücksichtigung folgender Punkte durchgeführt werden:

- a) die erforderlichen Fähigkeiten der Experten, die die Analyse durchführen;
- b) die Festlegung des Verfahrens für die Protokollanalyse;
- c) die erforderlichen Attribute für jedes sicherheitsrelevante Ereignis;
- d) Ausnahmen, die durch die Verwendung vorher festgelegter Regeln identifiziert werden [z. B. Sicherheitsinformations- und Ereignismanagement (SIEM) oder Firewall-Regeln und Einbruchserkennungssysteme (IDS, en: intrusion detection system) oder Schadsoftware-Signaturen];
- e) bekannte Verhaltensmuster und Standard-Netzwerkverkehr im Vergleich zu anomalen Aktivitäten und Verhalten [User and Entity Behaviour Analytics (UEBA)];
- f) Ergebnisse von Trend- oder Musteranalysen (z. B. als Ergebnis der Verwendung von Datenanalysen, Big-Data-Techniken und speziellen Analysetools);
- g) vorhandene Bedrohungsintelligenz.

Die Protokollanalyse sollte durch spezifische Überwachungsmaßnahmen unterstützt werden, um anomales Verhalten zu erkennen und zu analysieren:

- Überprüfung erfolgreicher und erfolgloser Zugriffsversuche auf geschützte Ressourcen [z. B. Domain Name System (DNS)-Server, Webportale und Dateifreigaben];
- Überprüfung von DNS-Protokollen, um ausgehende Netzwerkverbindungen zu böartigen Servern zu identifizieren, z. B. solche, die mit Botnet-Befehls- und Kontrollservern verbunden sind;
- Prüfung der Nutzungsberichte von Dienstleistern (z. B. Rechnungen oder Serviceberichte) auf ungewöhnliche Aktivitäten in Systemen und Netzen (z. B. durch Überprüfung von Aktivitätsmustern);
- einschließlich Ereignisprotokolle der physischen Überwachung wie Ein- und Ausgänge, um eine genauere Erkennung und Analyse von Vorfällen sicherzustellen;
- die Korrelation von Protokollen, um eine effiziente und hochgenaue Analyse zu ermöglichen.

Vermutete und tatsächliche Informationssicherheitsvorfälle sollten identifiziert werden (z. B. Infektion mit Schadsoftware oder Sondierung von Firewalls) und Gegenstand weiterer Untersuchungen sein (z. B. im Rahmen eines Prozesses zur Handhabung von Informationssicherheitsvorfällen, siehe 5.25).

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, kann erwogen werden, geeignete Dienstprogramme oder Audit-Werkzeuge zur Durchführung einer Dateiabfrage zu verwenden.

Die Ereignisprotokollierung bildet den Grundstein für automatisierte Überwachungssysteme (siehe 8.16), die in der Lage sind, konsolidierte Berichte und Warnungen zur Systemsicherheit zu erzeugen.

Ein SIEM-Tool oder ein gleichwertiger Dienst kann verwendet werden, um Protokolldaten zu speichern, zu korrelieren, zu normalisieren und zu analysieren und um Warnmeldungen zu generieren. SIEMs erfordern in der Regel eine sorgfältige Konfiguration, um ihren Nutzen zu optimieren. Zu den zu berücksichtigenden Konfigurationen gehören die Identifizierung und Auswahl geeigneter Protokollquellen, die Abstimmung und Prüfung von Regeln und die Entwicklung von Anwendungsfällen.

Öffentliche Transparenzdateien für die Aufzeichnung von Protokollen werden z. B. in Systemen der Zertifikatstransparenz verwendet. Solche Dateien können einen zusätzlichen Erkennungsmechanismus bieten, der zum Schutz vor Protokollmanipulationen nützlich ist.

In Cloud-Umgebungen können die Verantwortlichkeiten für das Protokollmanagement zwischen dem Cloud-Service-Kunden und dem Cloud-Service-Anbieter aufgeteilt werden. Die Verantwortlichkeiten variieren je nach Art des genutzten Cloud-Dienstes. Weitere Leitfäden sind in ISO/IEC 27017 zu finden.

8.16 Überwachung von Aktivitäten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Detektiv	#Vertraulichkeit	#Erkennen	#Handhabung von Informations sicherheitsereignissen	#Verteidigung
#Korrektiv	#Integrität #Verfügbarkeit	#Reagieren		

Maßnahme

Netzwerke, Systeme und Anwendungen sollten auf anormales Verhalten überwacht und geeignete Maßnahmen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.

Zweck

Erkennen von anormalem Verhalten und potentiellen Informationssicherheitsvorfällen.

Leitfaden

Umfang und Stufe der Überwachung sollten in Übereinstimmung mit den Geschäfts- und Informations-sicherheitsanforderungen und unter Berücksichtigung der einschlägigen Gesetze und Vorschriften festgelegt werden. Die Überwachungsaufzeichnungen sollten über einen bestimmten Zeitraum aufbewahrt werden.

Die folgenden Punkte sollten in das Überwachungssystem aufgenommen werden:

- a) ausgehender und eingehender Netzwerk-, System- und Anwendungsverkehr;
- b) Zugang zu Systemen, Servern, Netzwerkausrüstungen, Überwachungssystemen, kritischen Anwendungen, usw.;
- c) System- und Netzwerkkonfigurationsdateien auf kritischer oder administrativer Ebene;
- d) Protokolle von Sicherheitstools [z. B. Antivirus, IDS, Einbruchmeldeanlagen (IPS, en: intrusion prevention system), Webfilter, Firewalls, Verhinderung von Datenlecks];
- e) Ereignisprotokolle zu System- und Netzwerkaktivitäten;
- f) Überprüfung, ob der auszuführende Code im System laufen darf und ob er nicht manipuliert wurde (z. B. durch Neukompilierung, um einen zusätzlichen unerwünschten Code hinzuzufügen);
- g) Nutzung der Ressourcen (z. B. Prozessor, Festplatten, Speicher, Bandbreite) und deren Leistung.

Die Organisation sollte eine Ausgangsbasis für normales Verhalten festlegen und diese Ausgangsbasis auf Anomalien hin überwachen. Bei der Festlegung einer Ausgangsbasis sollten folgende Punkte berücksichtigt werden:

- a) Überprüfung der Auslastung der Systeme zu normalen und Spitzenzeiten;
- b) üblicher Zeitpunkt des Zugangs, Ort des Zugangs, Häufigkeit des Zugangs für jeden Benutzer oder jede Gruppe von Benutzern.

Das Überwachungssystem sollte anhand der festgelegten Ausgangsbasis konfiguriert werden, um anomales Verhalten zu erkennen, wie z. B.:

- a) ungeplante Beendigung von Prozessen oder Anwendungen;
- b) Aktivitäten, die typischerweise mit Schadsoftware in Verbindung gebracht werden, oder Datenverkehr, der von bekannten böartigen IP-Adressen oder Netzwerkdomänen ausgeht (z. B. solche, die mit Botnet-Befehls- und Kontrollservern verbunden sind);
- c) bekannte Angriffsmerkmale (z. B. Denial-of-Service und Pufferüberläufe);
- d) ungewöhnliches Systemverhalten (z. B. Aufzeichnung von Tastatureingaben, Prozessinjektion und Abweichungen bei der Verwendung von Standardprotokollen);

- e) Engpässe und Überlastungen (z. B. Netzwarteschlangen, Latenzzeiten und Netzjitter);
- f) unbefugter (tatsächlicher oder versuchter) Zugriff auf Systeme oder Informationen;
- g) unbefugtes Scannen von Geschäftsanwendungen, Systemen und Netzwerken;
- h) erfolgreiche und erfolglose Zugriffsversuche auf geschützte Ressourcen (z. B. DNS-Server, Webportale und Dateisysteme);
- i) ungewöhnliches Benutzer- und Systemverhalten im Verhältnis zum erwarteten Verhalten.

Es sollte eine kontinuierliche Überwachung mit Hilfe eines Überwachungsinstruments durchgeführt werden. Die Überwachung sollte in Echtzeit oder in regelmäßigen Abständen erfolgen, je nach Bedarf und Möglichkeiten der Organisation. Überwachungswerkzeuge sollten in der Lage sein, große Datenmengen zu verarbeiten, sich an eine sich ständig verändernde Bedrohungslandschaft anzupassen und eine Benachrichtigung in Echtzeit zu ermöglichen. Die Tools sollten auch in der Lage sein, bestimmte Signaturen und Daten oder Netz- und Anwendungsverhaltensmuster zu erkennen.

Automatisierte Überwachungssoftware sollte so konfiguriert sein, dass sie Warnmeldungen (z. B. über Verwaltungskonsolen, E-Mail-Nachrichten oder Instant-Messaging-Systeme) auf der Grundlage vordefinierter Schwellenwerte erzeugt. Das Warnsystem sollte auf die Ausgangslage der Organisation abgestimmt und optimiert werden, um Fehlalarme zu minimieren. Das Personal sollte für die Reaktion auf Warnmeldungen vorgesehen und entsprechend geschult sein, um mögliche Vorfälle richtig zu interpretieren. Es sollten redundante Systeme und Prozesse vorhanden sein, um Warnmeldungen zu empfangen und darauf zu reagieren.

Ungewöhnliche Ereignisse sollten den betroffenen Parteien mitgeteilt werden, um die folgenden Aktivitäten zu verbessern: Audit, Sicherheitsbewertung, Schwachstellen-Scanning und Überwachung (siehe 5.25). Es sollten Verfahren vorhanden sein, um auf positive Indikatoren des Überwachungssystems rechtzeitig zu reagieren, um die Auswirkungen von Vorfällen (siehe 5.26) auf die Informationssicherheit zu minimieren. Es sollten auch Verfahren zur Erkennung und Beseitigung von Fehlalarmen festgelegt werden, einschließlich der Einstellung der Überwachungssoftware, um die Zahl der künftigen Fehlalarme zu verringern.

Weitere Informationen

Die Sicherheitsüberwachung kann verbessert werden durch:

- a) Inanspruchnahme von Bedrohungsintelligenzsystemen (siehe 5.7);
- b) Einsatz von maschinellem Lernen und künstlicher Intelligenz;
- c) Verwendung von Block- oder Allowlists;
- d) Durchführung einer Reihe von technischen Sicherheitsbeurteilungen (z. B. Schwachstellenbeurteilungen, Penetrationstests, Simulationen von Cyberangriffen und Cyberreaktionsübungen) und Verwendung der Ergebnisse dieser Beurteilungen zur Festlegung von Grundlinien oder annehmbaren Verhaltensweisen;
- e) Einsatz von Leistungsüberwachungssystemen zur Feststellung und Erkennung von anormalem Verhalten;
- f) Inanspruchnahme von Protokollen in Kombination mit Überwachungssystemen.

Die Überwachung erfolgt häufig mit Hilfe spezieller Software, z. B. mit Angriffserkennungssystemen. Diese können auf der Grundlage normaler, annehmbarer und erwarteter System- und Netzwerkaktivitäten konfiguriert werden.

Die Überwachung anomaler Kommunikation hilft bei der Identifizierung von Botnetzen (d. h. einer Reihe von Geräten, die unter der böswilligen Kontrolle des Botnetzbesitzers stehen und in der Regel für verteilte Denial-of-Service-Angriffe auf andere Computer anderer Organisationen verwendet werden). Wenn der Computer von einem externen Gerät gesteuert wird, findet eine Kommunikation zwischen dem infizierten Gerät und dem Steuergerät statt. Die Organisation sollte daher Technologien einsetzen, um anomale Kommunikationen zu überwachen und gegebenenfalls entsprechende Maßnahmen zu ergreifen.

8.17 Uhrensynchronisation

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Detektiv	#Integrität	#Schützen #Erkennen	#Handhabung_von_Informationssicherheitsereignissen	#Schutz #Verteidigung

Maßnahme

Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme sollten mit zugelassenen Zeitquellen synchronisiert werden.

Zweck

Ermöglichung der Korrelation und Analyse von sicherheitsrelevanten Ereignissen und anderen aufgezeichneten Daten sowie Unterstützung der Untersuchung von Vorfällen im Bereich der Informationssicherheit.

Leitfaden

Die externen und internen Anforderungen an Zeitdarstellung, zuverlässige Synchronisation und Genauigkeit sollten dokumentiert und umgesetzt werden. Solche Anforderungen können sich aus rechtlichen, gesetzlichen, regulatorischen, vertraglichen, normativen und internen Überwachungserfordernissen ergeben. Für alle Systeme, einschließlich Gebäudemanagementsysteme, Eingangs- und Ausgangssysteme und andere Systeme, die zur Unterstützung von Untersuchungen herangezogen werden können, sollte eine standardisierte Referenz-Zeit zur Verwendung innerhalb der Organisation festgelegt und berücksichtigt werden.

Als Referenzuhr für die Protokollierungssysteme sollte eine Uhr verwendet werden, die mit einer per Funk ausgestrahlten nationalen Atomuhr oder dem Global Positioning System (GPS) verbunden ist; eine konsistente, vertrauenswürdige Datums- und Zeitquelle, die genaue Zeitstempel sicherstellt. Protokolle wie das Network Time Protocol (NTP) oder das Precision Time Protocol (PTP) sollten verwendet werden, um alle vernetzten Systeme mit einer Referenzuhr zu synchronisieren.

Die Organisation kann zwei externe Zeitquellen gleichzeitig nutzen, um die Zuverlässigkeit der externen Uhren zu verbessern und Abweichungen angemessen zu verwalten.

Die Synchronisierung der Uhr kann schwierig sein, wenn mehrere Cloud-Dienste verwendet werden oder wenn sowohl Cloud- als auch lokale Dienste genutzt werden. In diesem Fall sollten die Uhrzeiten der einzelnen Dienste überwacht und die Differenz aufgezeichnet werden, um Risiken aufgrund von Unstimmigkeiten zu mindern.

Weitere Informationen

Die korrekte Einstellung der Computeruhren ist wichtig, um die Genauigkeit von Ereignisprotokollen sicherzustellen, die für Untersuchungen oder als Beweisstück in Rechts- oder Maßregelungsfällen benötigt werden können. Ungenaue Audit-Protokolle können derartige Untersuchungen behindern und der Glaubwürdigkeit derartiger Beweisstücke schaden.

8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit #Sichere_Konfiguration #Anwendungssicherheit	#Schutz

Maßnahme

Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, sollte eingeschränkt und streng überwacht werden.

Zweck

Es wird sichergestellt, dass die Verwendung von Dienstprogrammen die System- und Anwendungsschutzmaßnahmen für die Informationssicherheit nicht beeinträchtigt.

Leitfaden

Die folgenden Leitfäden für die Verwendung von Dienstprogrammen, mit denen System- und Anwendungsschutzmaßnahmen außer Kraft gesetzt werden können, sollten beachtet werden:

- Beschränkung der Verwendung von Dienstprogrammen auf eine möglichst geringe Zahl vertrauenswürdiger, befugter Benutzer (siehe 8.2);
- Verwendung von Identifizierungs-, Authentifizierungs- und Genehmigungsverfahren für Dienstprogramme; einschließlich der eindeutigen Identifizierung der Person, die das Dienstprogramm nutzt;
- Festlegung und Dokumentation von Berechtigungsstufen für Dienstprogramme;
- Genehmigung zur Ad-hoc-Verwendung von Dienstprogrammen;
- Sperrung von Dienstprogrammen für Benutzer, die Zugang zu Anwendungen auf Systemen haben, bei denen eine Aufgabentrennung erforderlich ist;
- Entfernung bzw. Deaktivierung aller nicht notwendiger Dienstprogramme;
- zumindest eine logische Trennung der Dienstprogramme von der Anwendungssoftware. Wo dies möglich ist, sollte die Netzwerkkommunikation für solche Programme vom Anwendungsverkehr getrennt werden;
- Beschränkung der Verfügbarkeit von Dienstprogrammen (z. B. für die Dauer einer berechtigten Änderung);
- Protokollierung jeder Verwendung von Dienstprogrammen.

Weitere Informationen

Die meisten Informationssysteme verfügen über ein oder mehrere Dienstprogramme, die in der Lage sind, System- und Anwendungsschutzmaßnahmen außer Kraft zu setzen, z. B. Diagnose-, Patching-, Antivirus-, Festplattendefragmentierungs-, Debugger-, Sicherungs- und Netzwerkwerkzeuge.

8.19 Installation von Software auf Systemen im Betrieb

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration #Anwendungssicherheit	#Schutz

Maßnahme

Es sollten Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.

Zweck

Die Integrität von Systemen im Betrieb ist sichergestellt und die Ausnutzung technischer Schwachstellen unterbunden.

Leitfaden

Die folgenden Leitlinien sollten berücksichtigt werden, um Änderungen und Installationen von Software auf Betriebssystemen sicher zu verwalten:

- Durchführung von Aktualisierungen der Betriebssoftware nur durch geschulte Administratoren nach entsprechender Genehmigung durch das Management (siehe 8.5);
- Sicherstellung, dass nur genehmigter ausführbarer Code und kein Entwicklungscode oder Compiler auf betrieblichen Systemen installiert wird;
- die Installation und Aktualisierung von Software erst nach umfangreichen und erfolgreichen Prüfungen (siehe 8.29 und 8.31);
- die Aktualisierung aller zugehörigen Programmquellbibliotheken;
- Verwendung eines Konfigurationskontrollsystems, um die Kontrolle über die gesamte Betriebssoftware und die Systemdokumentation zu behalten;
- vor der Umsetzung der Änderungen Festlegung einer Rollback-Strategie;
- Führung eines Prüfprotokolls über alle Aktualisierungen der Betriebssoftware;
- Archivierung alter Softwareversionen zusammen mit allen erforderlichen Informationen und Parametern, Verfahren, Konfigurationsdetails und unterstützender Software als Notfallmaßnahme und solange die Software benötigt wird, um archivierte Daten zu lesen oder zu verarbeiten.

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 Schwachstellen hinsichtlich der Informationssicherheit, von der die aktuelle Version betroffen ist). Software-Patches sollten angewendet werden, wenn sie dazu beitragen, Schwachstellen hinsichtlich der Informationssicherheit zu beheben oder zu mindern (siehe 8.8 und 8.19).

Computersoftware kann von extern beschaffter Software und Paketen abhängig sein (z. B. Softwareprogramme mit Modulen, die auf externen Websites gehostet werden), die überwacht und kontrolliert werden sollten, um unbefugte Veränderungen zu vermeiden, da sie zu Schwachstellen in der Informationssicherheit führen können.

Anbietersoftware, die auf den Systemen im Betrieb 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. Open-Source-Software, die auf den Systemen im Betrieb verwendet wird, sollte auf dem neuesten Stand gehalten werden. Open-Source-Code kann im Laufe der Zeit nicht mehr gepflegt werden, ist aber weiterhin in einem Open-Source-Software-Repository verfügbar. Die Organisation sollte auch die Risiken berücksichtigen, die entstehen, wenn sie sich auf nicht gewartete Open-Source-Software verlässt, die auf den Systemen im Betrieb eingesetzt wird.

Wenn Lieferanten an der Installation oder Aktualisierung von Software beteiligt sind, sollte der physische oder logische Zugang nur bei Bedarf und mit entsprechender Genehmigung gewährt werden. Die Aktivitäten des Lieferanten sollten überwacht werden (siehe 5.22).

Die Organisation sollte strenge Regeln in Bezug auf die Art von Software festlegen und umsetzen, die von Anwendern installiert werden kann.

Bei der Installation von Software auf Betriebssystemen sollte das „Least Privilege“-Prinzip angewendet werden. 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 anhand der Funktionen der jeweiligen Anwender erfolgen.

Weitere Informationen

Keine weiteren Informationen.

8.20 Netzwerksicherheit

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz
#Detektiv	#Integrität #Verfügbarkeit	#Erkennen		

Maßnahme

Netzwerke und Netzwerkgeräte sollten gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.

Zweck

Schutz von Informationen in Netzwerken und den sie unterstützenden Informationsverarbeitungseinrichtungen vor Kompromittierung über das Netzwerk.

Leitfaden

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) die Art und die Klassifizierungsstufe der Informationen, die das Netzwerk unterstützen kann;
- b) Festlegung der Verantwortlichkeiten und Verfahren für die Verwaltung der Netzwerktechnik und Geräte;
- c) Pflege einer aktuellen Dokumentation, einschließlich Netzwerkdiagrammen und Konfigurationsdateien von Geräten (z. B. Router, Switches);
- d) gegebenenfalls Trennung der betrieblichen Verantwortlichkeit für die Netzwerke vom Betrieb der IKT-Systeme (siehe 5.3);
- e) Einrichtung von Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Daten, die über öffentliche Netze, Netze Dritter oder über drahtlose Netzwerke übertragen werden, und zum Schutz der angeschlossenen Systeme und Anwendungen (siehe 5.22, 8.24, 5.14 und 6.6). Zusätzliche Kontrollen können auch erforderlich sein, um die Verfügbarkeit der Netzwerkdienste und der an das Netzwerk angeschlossenen Computer sicherzustellen;
- f) angemessene Protokollierung und Überwachung, um die Aufzeichnung und Erkennung von Handlungen zu ermöglichen, die sich auf die Informationssicherheit auswirken können oder für diese relevant sind (siehe 8.16 und 8.15);
- g) enge Koordinierung der Netzverwaltungstätigkeiten, um den Dienst für die Organisation zu optimieren und sicherzustellen, dass die Maßnahmen in der gesamten Informationsverarbeitungsinfrastruktur einheitlich angewendet werden;
- h) die Authentifizierung von Systemen im Netzwerk;
- i) Einschränkung und Filterung der Verbindung von Systemen zum Netzwerk (z. B. durch Firewalls);
- j) Erkennung, Einschränkung und Authentifizierung des Anschlusses von Einrichtungen und Geräten an das Netzwerk;
- k) Absicherung von Netzwerkgeräten;
- l) Trennung der Netzverwaltungskanäle vom übrigen Netzwerkverkehr;
- m) vorübergehende Isolierung kritischer Teilnetze (z. B. mit Zugbrücken), wenn das Netzwerk angegriffen wird;
- n) Deaktivierung anfälliger Netzwerkprotokolle.

Die Organisation sollte sicherstellen, dass angemessene Sicherheitsmaßnahmen für die Nutzung virtualisierter Netzwerke getroffen werden. Virtualisierte Netzwerke umfassen auch Software-definierte Netzwerke (SDN, SD-WAN). Virtualisierte Netzwerke können unter Sicherheitsaspekten wünschenswert sein, da sie eine logische Trennung der über physische Netze stattfindenden Kommunikation ermöglichen, insbesondere für Systeme und Anwendungen, die mit verteilter Datenverarbeitung implementiert werden.

Weitere Informationen

Zusätzliche Informationen zur Netzwerksicherheit sind in der Normenreihe ISO/IEC 27033 zu finden.

Weitere Informationen zu virtualisierten Netzwerken sind in ISO/IEC TS 23167 zu finden.

8.21 Sicherheit von Netzwerkdiensten

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz

Maßnahme

Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste sollten ermittelt, umgesetzt und überwacht werden.

Zweck

Sicherstellung der Sicherheit bei der Nutzung von Netzwerkdiensten.

Leitfaden

Die für bestimmte Dienste erforderlichen Sicherheitsmaßnahmen wie Sicherheitsfunktionen, Dienstgüte (Service-Level) und Dienstanforderungen sollten festgestellt und (von internen oder externen Netzwerkdienstleistern) umgesetzt werden. Die Organisation sollte sicherstellen, dass die Anbieter von Netzwerkdiensten diese Maßnahmen umsetzen.

Die Fähigkeit des Bereitstellers von Netzwerkdiensten, die vereinbarten Dienste auf sichere Weise zu erbringen, sollte bestimmt und regelmäßig überwacht werden. Das Recht auf ein Audit sollte zwischen der Organisation und dem Anbieter vereinbart werden. Die Organisation sollte auch Bescheinigungen von Drittanbietern berücksichtigen, um nachzuweisen, dass sie angemessene Sicherheitsmaßnahmen anwenden.

Es sollten Regeln für die Nutzung von Netzwerken und Netzwerkdiensten formuliert und umgesetzt werden, um diese zu erfassen:

- die Netzwerke und Netzwerkdienste, zu denen Zugang gewährt wird;
- Anforderungen bezüglich der Authentifizierung für den Zugang zu verschiedenen Netzwerkdiensten;
- Genehmigungsverfahren zum Festlegen wem Zugang zu welchen Netzwerken und Netzwerkdiensten gewährt wird;
- Netzwerkmanagement sowie technische Maßnahmen und Verfahren zum Schutz des Zugangs zu Netzwerkverbindungen und Netzwerkdiensten;
- die verwendeten Mittel für den Zugang zu Netzwerken und Netzwerkdiensten (z. B. die Nutzung eines virtuellen privaten Netzes VPN oder WLAN);
- Zeit, Ort und andere Attribute des Benutzers zum Zeitpunkt des Zugriffs;
- Überwachung der Nutzung von Netzwerkdiensten.

Die folgenden Sicherheitsmerkmale von Netzwerkdiensten sollten berücksichtigt werden:

- 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) die Zwischenspeicherung (z. B. in einem Netzwerk für die Bereitstellung von Inhalten) und ihre Parameter, die es den Nutzern ermöglichen, die Nutzung der Zwischenspeicherung entsprechend den Anforderungen an Leistung, Verfügbarkeit und Vertraulichkeit zu wählen;
- d) Verfahren für die Nutzung der Netzwerkdienste zur ggf. erforderlichen Einschränkung des Zugriffs auf Netzwerkdienste oder Anwendungen.

Weitere Informationen

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

Weitere Leitlinien über ein Rahmenwerk für die Zugangsverwaltung sind in ISO/IEC 29146 enthalten.

8.22 Trennung von Netzwerken

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz

Maßnahme

Informationsdienste, Benutzer und Informationssysteme sollten in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.

Zweck

Aufteilung des Netzwerkes in Sicherheitsgrenzen und Kontrolle des Datenverkehrs zwischen diesen Grenzen auf der Grundlage der Geschäftsanforderungen.

Leitfaden

Die Organisation sollte in Erwägung ziehen, die Sicherheit großer Netzwerke zu verwalten, indem sie diese in separate Netzwerkdomänen aufteilt und sie vom öffentlichen Netzwerk (d. h. dem Internet) trennt. Diese Domänen können anhand der Vertrauens-, Kritikalitäts- und Sensibilitätsstufe (z. B. Domäne für öffentlichen Zugang, Desktop-Domäne, Server-Domäne, Systeme mit niedrigem und hohem Risiko), 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 realisiert werden.

Der Bereich jeder einzelnen Domäne sollte genau definiert werden. Wenn der domänenübergreifende Zugang gestattet ist, sollte er mittels eines Gateways (z. B. Firewall, filternder Router) gesteuert 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 themenspezifischen Richtlinie zur Zugangssteuerung (siehe 5.15), den Zugangsanforderungen, dem Wert und der Klassifizierung der verarbeiteten Informationen erfolgen, wobei 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. Die Anpassung der Funkabdeckung sollte für die Trennung der drahtlosen Netzwerke in Betracht gezogen werden. In sensiblen Umgebungen sollte darauf geachtet werden, alle Drahtloszugriffe wie externe Verbindungen zu behandeln und diesen Zugriff von den internen Netzwerken zu trennen, bis das Gateway entsprechend der Netzwerkkontrolle (siehe 8.20) passiert wurde, um erst dann den Zugriff auf die internen Systeme zu gewähren. Drahtlose Zugangsnetze für Gäste sollten von denen für das Personal getrennt werden, wenn das Personal nur kontrollierte Benutzerendgeräte verwendet, die mit den themenspezifischen Richtlinien der Organisation übereinstimmen. Für die Nutzung des Gäste-WLAN sollten mindestens die gleichen Einschränkungen gelten wie für das WLAN des Personals, um die Nutzung des Gäste-WLAN durch das Personal zu verhindern.

Weitere Informationen

Netzwerke erstrecken sich häufig über die Grenzen von Organisationen hinweg, 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 unbefugten 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.

8.23 Webfilterung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz

Maßnahme

Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.

Zweck

Schutz der Systeme vor dem Eindringen von Schadsoftware und Verhinderung des Zugriffs auf nicht autorisierte Webressourcen.

Leitfaden

Die Organisation sollte das Risiko verringern, dass ihre Mitarbeiter auf Websites zugreifen, die illegale Informationen enthalten oder dafür bekannt sind, dass sie Viren oder Phishing-Material bergen. Eine Technik, mit der dies erreicht werden kann, besteht darin, die IP-Adresse oder die Domäne der betreffenden Website(s) zu sperren. Einige Browser und Technologien zum Schutz vor Schadsoftware tun dies automatisch oder können so konfiguriert werden, dass sie dies tun.

Die Organisation sollte festlegen, zu welchen Arten von Websites das Personal Zugang haben sollte und zu welchen nicht. Die Organisation sollte in Erwägung ziehen, den Zugriff auf die folgenden Arten von Websites zu sperren:

- a) Websites, die über eine Funktion zum Hochladen von Informationen verfügen, es sei denn, dies ist aus triftigen geschäftlichen Gründen zulässig;
- b) bekannte oder vermutete bösartige Websites (z. B. solche, die Schadsoftware oder Phishing-Inhalte verbreiten);
- c) Befehls- und Steuerungsserver;
- d) bösartige Website, die aus Bedrohungsdaten gewonnen wurde (siehe 5.7);
- e) Websites mit illegalen Inhalten.

Bevor diese Maßnahme eingeführt wird, sollte die Organisation Regeln für die sichere und angemessene Nutzung von Online-Ressourcen aufstellen, einschließlich der Beschränkung auf unerwünschte oder ungeeignete Websites und webbasierte Anwendungen. Die Regeln sollten auf dem neuesten Stand gehalten werden.

Das Personal sollte in der sicheren und angemessenen Nutzung von Online-Ressourcen, einschließlich des Zugangs zum Internet, geschult werden. Die Schulung sollte die Regeln der Organisation, die Kontaktstelle für die Meldung von Sicherheitsbedenken und das Ausnahmeverfahren für den Fall umfassen, dass der Zugriff auf eingeschränkte Webressourcen aus legitimen geschäftlichen Gründen erforderlich ist. Das Personal sollte auch geschult werden, um sicherzustellen, dass es sich nicht über Browser-Hinweise hinwegsetzt, die melden, dass eine Website nicht sicher ist, und dem Benutzer trotzdem erlauben, fortzufahren.

Weitere Informationen

Die Webfilterung kann eine Reihe von Techniken umfassen, darunter Signaturen, Heuristiken, eine Liste zulässiger Websites oder Domänen, eine Liste verbotener Websites oder Domänen und eine maßgeschneiderte Konfiguration, um zu verhindern, dass bösartige Software und andere bösartige Aktivitäten das Netzwerk und die Systeme der Organisation angreifen.

8.24 Verwendung von Kryptographie

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration	#Schutz

Maßnahme

Es sollten Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.

Zweck

Sicherstellung des angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen nach den Anforderungen des Unternehmens und der Informationssicherheit und unter Berücksichtigung der rechtlichen, gesetzlichen, behördlichen und vertraglichen Anforderungen in Bezug auf Kryptographie.

Leitfaden

Allgemeines

Bei Gebrauch von Kryptographie sollten folgende Punkte berücksichtigt werden:

- a) die von der Organisation festgelegte themenspezifische Richtlinie zur Kryptographie, einschließlich der allgemeinen Grundsätze für den Schutz von Informationen. Eine themenspezifische Richtlinie für den Einsatz von Kryptographie ist notwendig, um die Vorteile des Einsatzes von Verschlüsselungsverfahren voll auszuschöpfen, die damit verbundenen Risiken möglichst gering zu halten und einen unangemessenen oder unsachgemäßen Gebrauch zu vermeiden;
- b) Identifizierung der erforderlichen Schutzstufe und der Klassifizierung der Informationen und folglich Festlegung der Art, Stärke und Qualität der erforderlichen kryptographischen Algorithmen;
- c) die Verwendung von Kryptographie zum Schutz von Informationen, die sich auf Endpunktgeräten oder Speichermedien mobiler Nutzer befinden und über Netze an solche Geräte oder Speichermedien übertragen werden;
- d) der Ansatz zur Verwaltung kryptographischer Schlüssel, einschließlich Verfahren zur Handhabung der Erzeugung und des Schutzes kryptographischer Schlüssel und der Wiederherstellung verschlüsselter Daten im Falle verlorener, kompromittierter oder beschädigter Schlüssel;
- e) Aufgaben und Verantwortlichkeiten für:
 - 1) die Umsetzung der Regeln für den wirksamen Einsatz der Kryptographie;
 - 2) die Verwaltung der Schlüssel, einschließlich deren Erzeugung (siehe 8.24);
- f) die anzunehmenden Normen sowie die kryptographischen Algorithmen, die Verschlüsselungsstärke, die kryptographischen Lösungen und die Verwendungspraktiken, die für die Verwendung in der Organisation zugelassen oder erforderlich sind;
- g) die Auswirkung der Verwendung verschlüsselter Daten auf Maßnahmen, die auf der Überprüfung von Inhalten basieren (z. B. Schadsoftware-Erkennung oder Inhaltsfilterung).

Bei der Umsetzung der Regeln der Organisation für den effektiven Einsatz von Kryptographie sollten die Verordnungen und nationalen Beschränkungen, die für den Einsatz kryptographischer Techniken in verschiedenen Teilen der Welt gelten können, ebenso berücksichtigt werden wie die Fragen des grenzüberschreitenden Flusses verschlüsselter Informationen (siehe 5.31).

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 5.22) einschließen.

Schlüsselverwaltung

Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Erzeugung, Speicherung, Archivierung, Abruf, Verteilung, Deaktivierung und Löschung kryptographischer Schlüssel.

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 Frage, wie Schlüssel bei Erhalt zu aktivieren sind;
- d) zur Speicherung von Schlüsseln, einschließlich der Information, wie befugte Benutzer Zugang zu diesen erhalten;
- e) zur Änderung oder Aktualisierung von Schlüsseln, einschließlich der Regeln, wann und wie die Schlüssel zu ändern sind;
- f) zum Umgang mit kompromittierten Schlüsseln;
- g) Widerruf von Schlüsseln, einschließlich der Frage, wie man Schlüssel zurückziehen oder deaktivieren kann [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 der Schlüsselverwaltung betreffender Aktivitäten;
- l) Festlegung von Aktivierungs- und Deaktivierungsdaten für Schlüssel, damit die Schlüssel nur für den Zeitraum verwendet werden können, der in den Regeln der Organisation für die Schlüsselverwaltung vorgesehen ist;
- m) Umgang mit gerichtlichen Aufforderungen bezüglich des Zugangs auf kryptographische Schlüssel (z. B. kann es erforderlich sein, verschlüsselte Daten in unverschlüsselter Form als Beweismittel für eine Gerichtsverhandlung verfügbar zu machen).

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.

Zusätzlich sollte zur Integrität für viele Anwendungsfälle auch die Authentizität der öffentlichen Schlüssel berücksichtigt werden.

Weitere Informationen

Die Authentizität öffentlicher Schlüssel wird in der Regel durch Verfahren zur Verwaltung öffentlicher Schlüssel unter Verwendung von Zertifizierungsstellen und Zertifikaten für öffentliche Schlüssel sichergestellt, aber es ist auch möglich, dies durch den Einsatz von Technologien zu erreichen, z. B. durch die Anwendung manueller Verfahren für Schlüssel mit geringer Anzahl.

Kryptographie kann dazu verwendet werden, verschiedene Informationssicherheitsziele zu erreichen, z. B.:

- a) Vertraulichkeit: Gebrauch von Verschlüsselung zum Schutz sensibler oder betriebswichtiger, gespeicherter oder übertragener Daten;
- b) Integrität oder Authentizität: Verwendung digitaler Signaturen oder Authentifizierungscodes für Nachrichten zur Bestätigung der Authentizität bzw. Integrität gespeicherter oder übertragener sensibler oder betriebswichtiger Daten. Verwendung von Algorithmen für die Überprüfung der Dateintegrität;
- c) Unabstreitbarkeit: Gebrauch von Verschlüsselungsverfahren zum Nachweis des Eintritts bzw. Nichteintritts eines Ereignisses oder einer Handlung;
- d) Authentifizierung: Gebrauch von Verschlüsselungsverfahren zur Authentifizierung von Benutzern und anderen Systementitäten, die Zugang zu oder Transaktionen mit Systembenutzern, -entitäten und -ressourcen beantragen.

Die Normenreihe ISO/IEC 11770 enthält weitere Informationen zur Schlüsselverwaltung.

8.25 Lebenszyklus einer sicheren Entwicklung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Regeln für die sichere Entwicklung von Software und Systemen sollten festgelegt und angewendet werden.

Zweck

Es ist sichergestellt, dass Informationssicherheit im sicheren Entwicklungszyklus von Software und Systemen geplant und umgesetzt ist.

Leitfaden

Die sichere Entwicklung ist eine der Anforderungen zum Aufbau eines sicheren Dienstes, einer sicheren Architektur, einer Software bzw. eines sicheren Systems. Um dies zu erreichen, sollten die folgenden Gesichtspunkte berücksichtigt werden:

- a) Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen (siehe 8.31);
- b) Richtlinie bezüglich der Sicherheit im Softwareentwicklungsprozess;
 - 1) Sicherheit in der Softwareentwicklungsmethodik (siehe 8.28 und 8.27);
 - 2) Richtlinien zur sicheren Programmierung für jede verwendete Programmiersprache (siehe 8.28);
- c) Sicherheitsanforderungen in der Spezifikations- und Entwurfsphase (siehe 5.8);
- d) Sicherheitskontrollpunkte in Projekten (siehe 5.8);

- e) System- und Sicherheitsprüfung, wie Regressionsprüfung, Code-Scan und Penetrationstests (siehe 8.29);
- f) sichere Repositorien für Quellcode und Konfiguration (siehe 8.4 und 8.9);
- g) Sicherheit bei der Versionskontrolle (siehe 8.32);
- h) erforderliche Kenntnisse und Ausbildung im Bereich der Anwendungssicherheit (siehe 8.28);
- i) Fähigkeit der Entwickler, Schwachstellen zu verhindern, zu finden und zu beheben (siehe 8.28);
- j) Genehmigungsanforderungen und Alternativen, um kosteneffiziente Lösungen sicherzustellen und gleichzeitig künftige Genehmigungsprobleme zu vermeiden (siehe 5.32).

Wenn die Entwicklung ausgelagert wird, sollte die Organisation die Zusicherung verlangen, dass der Lieferant die Regeln der Organisation für sichere Entwicklung einhält (siehe 8.30).

Weitere Informationen

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

8.26 Anforderungen an die Anwendungssicherheit

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz #Verteidigung

Maßnahme

Die Anforderungen an die Informationssicherheit sollten bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.

Zweck

Sicherstellen, dass bei der Entwicklung oder Beschaffung von Anwendungen alle Anforderungen an die Informationssicherheit ermittelt und berücksichtigt werden.

Leitfaden

Allgemeines

Die Anforderungen an die Anwendungssicherheit sollten ermittelt und spezifiziert werden. Diese Anforderungen werden in der Regel durch eine Risikobeurteilung ermittelt. Die Anforderungen sollten mit der Unterstützung von Informationssicherheitsspezialisten entwickelt werden.

Die Anforderungen an die Anwendungssicherheit können je nach Zweck der Anwendung ein breites Spektrum an Themen abdecken.

Die Anforderungen an die Anwendungssicherheit sollten, soweit zutreffend, Folgendes umfassen:

- a) Stufe des Vertrauens in die Identität von Entitäten [z. B. durch Authentifizierung (siehe 5.17, 8.2 und 8.5)];
- b) Identifizierung der Art der Informationen und der Klassifizierungsstufe, die von der Anwendung verarbeitet werden soll;
- c) Notwendigkeit der Trennung des Zugangs und der Zugangsebene zu Daten und Funktionen in der Anwendung;
- d) Widerstandsfähigkeit gegen böswillige Angriffe oder unbeabsichtigte Störungen [z. B. Schutz vor Pufferüberlauf oder strukturierter Abfragesprache (SQL, en: structured query language)];
- e) rechtliche, gesetzliche und behördliche Anforderungen der Rechtsordnung, in der die Transaktion erzeugt, verarbeitet, abgeschlossen oder gespeichert wurde;
- f) das Bedürfnis nach Privatsphäre aller beteiligten Parteien;
- g) die Schutzanforderungen für vertrauliche Informationen;
- h) Schutz der Daten während der Verarbeitung, bei der Übertragung und im Ruhezustand;
- i) die Notwendigkeit, die Kommunikation zwischen allen beteiligten Parteien sicher zu verschlüsseln;
- j) Eingabesteuerungen, einschließlich Integritätsprüfungen und Eingabevalidierung;
- k) automatische Steuerungen (z. B. Genehmigungsgrenzen oder doppelte Genehmigungen);
- l) Ausgangssteuerungen, wobei auch zu berücksichtigen ist, wer auf die Ausgänge zugreifen kann und wer dazu berechtigt ist;
- m) Einschränkungen in Bezug auf den Inhalt von „Freitext“-Feldern, da diese zu einer unkontrollierten Speicherung vertraulicher Daten (z. B. personenbezogener Daten) führen können;
- n) die aus dem Geschäftsablauf abgeleiteten Anforderungen wie die Protokollierung und Überwachung von Transaktionen sowie Anforderungen bezüglich der Nichtabstreitbarkeit;
- o) die Anforderungen, die durch andere Sicherheitsmaßnahmen gegeben sind (z. B. Schnittstellen zu Protokollierungs- und Überwachungssystemen oder Systemen zur Erkennung von Datenverlusten);
- p) Umgang mit Fehlermeldungen.

Transaktionsbezogene Dienste

Bei Anwendungen, die transaktionsbezogene Dienste zwischen der Organisation und einem Partner anbieten, sollte bei der Ermittlung der Anforderungen an die Informationssicherheit außerdem Folgendes berücksichtigt werden:

- a) die Vertrauensstufe, die für eine Partei in Bezug auf die von einer anderen Partei angegebenen Identität erforderlich ist;
- b) die erforderliche Stufe des Vertrauens in die Integrität der ausgetauschten oder verarbeiteten Informationen und die Mechanismen zur Feststellung mangelnder Integrität (z. B. zyklische Redundanzprüfung, Hashing, digitale Signaturen);

- c) Genehmigungsprozesse im Zusammenhang mit der Frage, wer die Inhalte wichtiger Transaktionsdokumente genehmigen, diese herausgeben oder unterzeichnen kann;
- d) Vertraulichkeit, Integrität, den Nachweis des Versands und Erhalts wichtiger Dokumente und die Nichtabstreitbarkeit (z. B. von Verträgen in Verbindung mit Angebots- und Vertragsprozessen);
- e) die Vertraulichkeit und Integrität jedweder Transaktionen (z. B. Aufträge, Lieferadressen-Details und Empfangsbestätigungen);
- f) Anforderungen an die Dauer der Geheimhaltung einer Transaktion;
- g) Versicherung und andere vertragliche Anforderungen.

Elektronische Bestell- und Zahlungsanwendungen

Bei Anwendungen, die eine elektronische Bestellung und Bezahlung vorsehen, sollte außerdem Folgendes beachtet werden:

- a) Anforderungen an die Wahrung der Vertraulichkeit und Integrität der Auftragsdaten;
- b) der angemessene Aufwand zur Verifizierung der von einem Kunden angegebenen Zahlungsinformationen;
- c) Verhinderung von Verlust oder Vervielfältigung der Transaktionsinformationen;
- d) Speicherung der Transaktionsdaten an einem nicht öffentlich zugänglichen Ort (z. B. einer Storage-Plattform im Intranet der Organisation, und die Transaktionsdaten werden nicht auf elektronischen Speichermedien aufbewahrt und zur Verfügung gestellt, die direkt über das Internet zugänglich sind);
- e) 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.

Mehrere der oben genannten Überlegungen können durch die Anwendung von Kryptographie (siehe 8.24) unter Berücksichtigung der rechtlichen Anforderungen (siehe 5.31 bis 5.36, insbesondere 5.31 für Kryptographiegesetze) angesprochen werden.

Weitere Informationen

Anwendungen, auf die über Netze zugegriffen werden kann, sind einer Reihe netzbezogener Bedrohungen durch betrügerische Aktivitäten, Vertragsstreitigkeiten oder unrechtmäßige Veröffentlichung von Informationen, unvollständige Übermittlung, Fehlleitung, unbefugte Änderung von Nachrichten, Vervielfältigung oder Wiedergabe ausgesetzt. Daher sind eine ausführliche Risikoeinschätzung und eine sorgfältige Festlegung von Kontrollmaßnahmen unverzichtbar. Zu den erforderlichen Kontrollmaßnahmen gehören häufig Verschlüsselungsverfahren für die Authentifizierung und die sichere Datenübertragung.

Weitere Informationen zur Anwendungssicherheit können der Normenreihe ISO/IEC 27034 entnommen werden.

8.27 Sichere Systemarchitektur und technische Grundsätze

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sollten festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.

Zweck

Sicherstellung einer sicheren Konzeption, Implementierung und eines sicheren Betriebs von Informationssystemen im Rahmen des Entwicklungslebenszyklus.

Leitfaden

Die Grundsätze der Sicherheitstechnik sollten festgelegt, dokumentiert und bei der Entwicklung von Informationssystemen angewendet werden. Sicherheitsaspekte sollten bei der Entwicklung sämtlicher Architekturschichten (Geschäftsanforderungen, Daten, Anwendungen und Technologie) berücksichtigt werden. Neue Technologien sollten hinsichtlich ihrer Sicherheitsrisiken analysiert und der Entwurf mit Blick auf bekannte Angriffsmuster überprüft werden.

Die Grundsätze der Sicherheitstechnik bieten eine Anleitung für Benutzerauthentifizierungstechniken, eine sichere Sitzungssteuerung und Datenvalidierung sowie Bereinigung.

Die Grundsätze der sicheren Systemtechnik sollten die Analyse folgender Punkte umfassen:

- das gesamte Spektrum der Sicherheitsmaßnahmen, die erforderlich sind, um Informationen und Systeme gegen festgestellte Bedrohungen zu schützen;
- die Fähigkeiten der Sicherheitsmaßnahmen zur Verhinderung, Erkennung oder Reaktion auf Sicherheitsereignisse;
- spezifische Sicherheitsmaßnahmen, die für bestimmte Geschäftsprozesse erforderlich sind (z. B. Verschlüsselung sensibler Informationen, Integritätsprüfung und digitale Signierung von Informationen);
- wo und wie die Sicherheitsmaßnahmen anzuwenden sind (z. B. durch Integration mit einer Sicherheitsarchitektur und der technischen Infrastruktur);
- wie die einzelnen (manuellen und automatisierten) Sicherheitskontrollmaßnahmen zusammenwirken, um ein integriertes Paket von Maßnahmen zu schaffen.

Sicherheitstechnische Grundsätze sollten Folgendes berücksichtigen:

- die Notwendigkeit der Integration in eine Sicherheitsarchitektur;
- technische Sicherheitsinfrastruktur [z. B. Public-Key-Infrastruktur (PKI), Identitäts- und Zugangsverwaltung (IAM), Verhinderung von Datenlecks und dynamische Zugangsverwaltung];

- c) Fähigkeit der Organisation, die gewählte Technologie zu entwickeln und zu unterstützen;
- d) Kosten, Zeit und Komplexität der Erfüllung von Sicherheitsanforderungen;
- e) derzeitige bewährte Praktiken.

Sichere Systemtechnik sollte beinhalten:

- a) die Anwendung von Grundsätzen der Sicherheitsarchitektur wie „Sicherheit durch Gestaltung“, „Verteidigung in der Tiefe“, „Sicherheit durch Voreinstellung“, „Standardverweigerung“, „Ausfallsicherheit“, „Misstrauen gegenüber Eingaben von externen Anwendungen“, „Sicherheit bei der Bereitstellung“, „Annahme eines Verstoßes“, „geringstes Privileg“, „Benutzerfreundlichkeit und Verwaltbarkeit“ und „geringste Funktionalität“;
- b) eine sicherheitsorientierte Konzeptionsprüfung, die dazu beiträgt, Schwachstellen in der Informationssicherheit zu ermitteln und sicherzustellen, dass die Sicherheitsmaßnahmen spezifiziert sind und den Sicherheitsanforderungen entsprechen;
- c) Dokumentation und förmliche Bestätigung von Sicherheitsmaßnahmen, die die Anforderungen nicht vollständig erfüllen (z. B. aufgrund übergeordneter Sicherheitsanforderungen);
- d) Absicherung von Systemen.

Die Organisation sollte „Null-Vertrauen“-Grundsätze berücksichtigen, wie z. B.:

- a) in der Annahme, dass die Informationssysteme der Organisation bereits angegriffen wurden und man sich daher nicht allein auf die Sicherheit des Netzwerkperimeters verlassen kann;
- b) Anwendung eines Ansatzes „Niemals vertrauen, immer überprüfen“ (Zero-Trust-Ansatz) für den Zugang zu Informationssystemen;
- c) Sicherstellung, dass Anfragen an Informationssysteme von Anfang bis Ende verschlüsselt werden;
- d) Überprüfung jeder Anfrage an ein Informationssystem, als käme sie aus einem offenen, externen Netz, auch wenn diese Anfragen aus der Organisation selbst stammen (d. h. kein automatisches Vertrauen in alles, was innerhalb oder außerhalb der Grenzen der Organisation liegt);
- e) Anwendung von Techniken des „geringsten Privilegs“ (least privilege) und der dynamischen Zugangssteuerung (siehe 5.15, 5.18 und 8.2). Dazu gehört die Authentifizierung und Autorisierung von Anfragen nach Informationen oder an Systeme auf der Grundlage von Kontextinformationen wie Authentifizierungsinformationen (siehe 5.17), Benutzeridentitäten (siehe 5.16), Daten über das Endpunktgerät des Benutzers und Datenklassifizierung (siehe 5.12);
- f) die ständige Authentifizierung von Anforderern und die ständige Validierung von Genehmigungsanfragen an Informationssysteme auf der Grundlage von Informationen wie Authentifizierungsinformationen (siehe 5.17) und Benutzeridentitäten (siehe 5.16), Daten über das Endpunktgerät des Benutzers und Datenklassifizierung (siehe 5.12), z. B. die Durchsetzung einer starken Authentifizierung (z. B. Multifaktor, siehe 8.5).

Die festgelegten Grundsätze der sicheren Analyse, Entwicklung und Pflege sollten über die Verträge und anderen verbindlichen Vereinbarungen zwischen der Organisation und dem jeweiligen Outsourcing-Partner ggf. auch auf die ausgelagerte Entwicklung von Informationssystemen angewendet werden. Die Organisation sollte sicherstellen, dass die sicherheitstechnischen Praktiken der Lieferanten mit den Anforderungen der Organisation übereinstimmen.

Die Grundsätze der sicheren Analyse, Entwicklung und Pflege 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 potentieller Bedrohungen nach wie vor aktuell sind und dass sie an Fortschritte bei Technologien und Lösungen angepasst werden können.

Weitere Informationen

Die Grundsätze der Sicherheitstechnik können auf die Entwicklung oder Konfiguration einer Reihe von Techniken angewandt werden, z. B.:

- Fehlertoleranz und andere Ausfallsicherheitstechniken;
- Segregation (z. B. durch Virtualisierung oder Containerisierung);
- Manipulationssicherheit.

Sichere Virtualisierungstechniken können eingesetzt werden, um Störungen zwischen Anwendungen zu verhindern, die auf demselben physischen Gerät laufen. Wenn eine virtuelle Instanz einer Anwendung von einem Angreifer kompromittiert wird, ist nur diese Instanz betroffen. Der Angriff hat keine Auswirkungen auf andere Anwendungen oder Daten.

Manipulationssicherheitstechniken können eingesetzt werden, um die Manipulation von Informationsbehältern zu erkennen, unabhängig davon, ob es sich um physische (z. B. einen Einbruchalarm) oder logische (z. B. eine Datei) handelt. Ein Merkmal dieser Techniken ist, dass der Versuch, den Behälter zu manipulieren, aufgezeichnet wird. Darüber hinaus kann die Maßnahme die erfolgreiche Extraktion von Daten durch deren Zerstörung verhindern (z. B. kann der Gerätespeicher gelöscht werden).

8.28 Sicheres Coding

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.

Zweck

Sicherstellung, dass die Software sicher geschrieben wird, um die Anzahl der potentiellen Sicherheitslücken in der Software zu reduzieren.

Leitfaden

Allgemeines

Die Organisation sollte organisationsweite Prozesse einrichten, um eine gute Governance für sichere Codierung zu gewährleisten. Es sollte ein Mindestmaß an Sicherheit geschaffen und angewendet werden.

Darüber hinaus sollten diese Prozesse und die Governance auf Softwarekomponenten von Dritten und Open-Source-Software ausgeweitet werden.

Die Organisation sollte reale Bedrohungen sowie aktuelle Ratschläge und Informationen über Softwareschwachstellen überwachen, um die Grundsätze der sicheren Codierung der Organisation durch kontinuierliche Verbesserung und Lernen zu steuern. Auf diese Weise kann sichergestellt werden, dass wirksame Verfahren zur sicheren Codierung implementiert werden, um die sich schnell verändernde Bedrohungslandschaft zu bekämpfen.

Planung und Vorcodierung

Die Grundsätze der sicheren Codierung sollten sowohl bei Neuentwicklungen als auch bei Wiederverwendungsszenarien angewandt werden. Diese Grundsätze sollten auf die Entwicklungsaktivitäten sowohl innerhalb der Organisation als auch für Produkte und Dienstleistungen, die von der Organisation an andere geliefert werden, angewandt werden. Die Planung und die Voraussetzungen vor der Codierung sollten Folgendes umfassen:

- a) organisationsspezifische Erwartungen und anerkannte Grundsätze für sichere Codierung, die sowohl für interne als auch für ausgelagerte Code-Entwicklungen verwendet werden können;
- b) gängige und historische Codierungspraktiken und Fehler, die zu Schwachstellen in der Informationssicherheit führen;
- c) die Konfiguration von Entwicklungswerkzeugen, wie integrierten Entwicklungsumgebungen (IDE), um die Erstellung eines sicheren Codes zu erzwingen;
- d) entsprechend den von den Anbietern von Entwicklungswerkzeugen und Ausführungsumgebungen herausgegebenen Leitfäden, soweit zutreffend;
- e) Pflege und Einsatz aktueller Entwicklungswerkzeuge (z. B. Compiler);
- f) Qualifikation von Entwicklern beim Schreiben eines sicheren Codes;
- g) sichere Gestaltung und Architektur, einschließlich Bedrohungsmodellierung;
- h) sichere Programmierstandards und gegebenenfalls die Vorgabe ihrer Verwendung;
- i) Verwendung von kontrollierten Umgebungen für die Entwicklung.

Während der Codierung

Bei der Codierung sollten folgende Punkte berücksichtigt werden:

- a) sichere Codierungspraktiken, die für die verwendeten Programmiersprachen und -techniken spezifisch sind;
- b) Anwendung sicherer Programmiertechniken wie Pair Programming, Refactoring, Peer Review, Sicherheitsiterationen und testgestützte Entwicklung;
- c) Verwendung von Techniken der strukturierten Programmierung;
- d) die Dokumentation des Codes und die Beseitigung von Programmierfehlern, die die Ausnutzung von Schwachstellen in der Informationssicherheit ermöglichen können;
- e) Verbot der Verwendung unsicherer Gestaltungstechniken (z. B. die Verwendung von fest codierten Kennwörtern, nicht genehmigten Code-Mustern und nicht authentifizierten Webdiensten).

Die Prüfung sollte während und nach der Entwicklung durchgeführt werden (siehe 8.29). Statische Anwendungssicherheitstests (SAST) können Sicherheitsschwachstellen in Software aufdecken.

Bevor die Software in Betrieb genommen wird, sollten folgende Punkte bewertet werden:

- a) Angriffsfläche und das Prinzip der geringsten Privilegien;
- b) Durchführung einer Analyse der häufigsten Programmierfehler und Dokumentation, dass diese behoben wurden.

Überprüfung und Wartung

Nachdem der Code in Betrieb genommen wurde:

- a) Updates sollten sicher verpackt und eingesetzt werden;
- b) gemeldete Schwachstellen in der Informationssicherheit sollten behandelt werden (siehe 8.8);
- c) Fehler und vermutete Angriffe sollten protokolliert und die Protokolle regelmäßig überprüft werden, um gegebenenfalls Anpassungen am Code vorzunehmen;
- d) der Quellcode sollte vor unbefugtem Zugriff und Manipulationen geschützt werden (z. B. durch den Einsatz von Konfigurationsmanagement-Tools, die in der Regel Funktionen wie Zugangssteuerung und Versionskontrolle bieten).

Bei der Verwendung externer Tools und Bibliotheken sollte die Organisation Folgendes berücksichtigen:

- a) Sicherstellung, dass externe Bibliotheken verwaltet werden (z. B. durch Führung eines Inventars der verwendeten Bibliotheken und ihrer Versionen) und regelmäßig mit den Versionszyklen aktualisiert werden;
- b) Auswahl, Autorisierung und Wiederverwendung von gut geprüften Komponenten, insbesondere Authentifizierungs- und kryptographischen Komponenten;
- c) die Lizenz, die Sicherheit und die Historie der externen Komponenten;
- d) Sicherstellung, dass die Software wartbar und nachvollziehbar ist und aus bewährten, seriösen Quellen stammt;
- e) ausreichend langfristige Verfügbarkeit von Entwicklungsressourcen und Artefakten.

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) ob die Zustimmung des Anbieters eingeholt werden soll;
- 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.

Weitere Informationen

Ein Leitprinzip besteht darin, sicherzustellen, dass der sicherheitsrelevante Code bei Bedarf aufgerufen wird und manipulationssicher ist. Programme, die aus kompiliertem Binärcode installiert werden, verfügen ebenfalls über diese Eigenschaften, allerdings nur für die in der Anwendung enthaltenen Daten. Bei interpretierten Sprachen funktioniert das Konzept nur, wenn der Code auf einem Server ausgeführt wird, auf den die Benutzer und Prozesse, die ihn verwenden, nicht zugreifen können, und wenn die Daten in einer ähnlich geschützten Datenbank gespeichert sind. So kann der interpretierte Code beispielsweise auf einem Cloud-Dienst ausgeführt werden, für den der Zugriff auf den Code selbst Administratorrechte erfordert. Ein solcher Administratorenzugang sollte durch Sicherheitsmechanismen wie Just-in-Time-Verwaltungsprinzipien und starke Authentifizierung geschützt werden. Wenn der Eigentümer der Anwendung durch direkten Fernzugriff auf den Server auf Skripte zugreifen kann, kann dies im Prinzip auch ein Angreifer. Webserver sollten so konfiguriert werden, dass das Durchsuchen von Verzeichnissen in solchen Fällen verhindert wird.

Bei der Entwicklung des Anwendungscodes geht man am besten von der Annahme aus, dass er immer angegriffen werden kann, sei es durch Fehler oder böswillige Handlungen. Darüber hinaus können kritische Anwendungen so konzipiert werden, dass sie gegenüber internen Fehlern tolerant sind. So kann beispielsweise die Ausgabe eines komplexen Algorithmus überprüft werden, um sicherzustellen, dass sie innerhalb sicherer Grenzen liegt, bevor die Daten in einer Anwendung wie einer sicherheits- oder finanzkritischen Anwendung verwendet werden. Der Code, der die Grenzprüfungen durchführt, ist einfach und daher viel leichter auf Korrektheit zu prüfen.

Einige Webanwendungen sind anfällig für eine Reihe von Schwachstellen, die durch mangelhafte Gestaltung und Codierung verursacht werden, wie z. B. Datenbankinjektion und Cross-Site-Scripting-Angriffe. Bei diesen Angriffen können Anfragen manipuliert werden, um die Funktionalität des Webserverns zu missbrauchen.

Weitere Informationen zur IKT-Sicherheitsvaluierung können der Normenreihe ISO/IEC 15408 entnommen werden.

8.29 Sicherheitsprüfung in Entwicklung und Abnahme

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Anwendungssicherheit #Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Sicherheitsprüfverfahren sollten definiert und in den Entwicklungslebenszyklus integriert werden.

Zweck

Überprüfung, ob die Anforderungen an die Informationssicherheit erfüllt sind, wenn Anwendungen oder der Code in der Produktionsumgebung eingesetzt werden.

Leitfaden

Neue Informationssysteme, Upgrades und neue Versionen sollten während des Entwicklungsprozesses gründlich geprüft und verifiziert werden. Sicherheitsprüfungen sollten ein integraler Bestandteil der Prüfung von Systemen oder Komponenten sein.

Sicherheitsprüfungen sollten anhand einer Reihe von Anforderungen durchgeführt werden, die als funktional oder nicht-funktional ausgedrückt werden können. Die Sicherheitsprüfung sollte folgende Tests umfassen:

- a) Sicherheitsfunktionen [z. B. Benutzerauthentifizierung (siehe 8.5), Zugangsbeschränkung (siehe 8.3) und Einsatz von Kryptographie (siehe 8.24)];
- b) sichere Codierung (siehe 8.28);
- c) sichere Konfigurationen (siehe 8.9, 8.20 und 8.22), einschließlich der Betriebssysteme, Firewalls und anderer Sicherheitskomponenten.

Testpläne sollten anhand einer Reihe von Kriterien festgelegt werden. Der Umfang der Prüfungen sollte im Verhältnis zur Bedeutung, zur Art des Systems und zu den möglichen Auswirkungen der eingeführten Änderung stehen. Der Prüfplan sollte Folgendes enthalten:

- a) einen detaillierten Zeitplan für Aktivitäten und Prüfungen;
- b) Eingaben und erwartete Ergebnisse unter einer Reihe von Bedingungen;
- c) Kriterien zur Evaluierung der Ergebnisse;
- d) Entscheidung über weitere Maßnahmen, falls erforderlich.

Die Organisation kann sich automatischer Tools wie Codeanalyse-Tools oder Schwachsteller-Scanner bedienen und sollten sich von der Behebung sicherheitsbezogener Defizite überzeugen.

Wie bei internen Entwicklungsvorhaben sollten derartige Prüfungen zunächst vom Entwicklungsteam durchgeführt werden. Danach sollten unabhängige Abnahmeprüfungen unternommen werden, um sicherzustellen, dass das System wie erwartet (und nur wie erwartet) funktioniert (siehe 5.8). Folgendes sollte berücksichtigt werden:

- a) Durchführung von Code-Review-Aktivitäten als relevantes Element für die Prüfung auf Sicherheitsmängel, einschließlich unvorhergesehener Eingaben und Bedingungen;
- b) Durchführung von Schwachstellen-Scans zur Ermittlung unsicherer Konfigurationen und Systemschwachstellen;
- c) Durchführung von Penetrationstests zur Ermittlung von unsicherem Code und Design.

Für ausgelagerte Entwicklungs- und Beschaffungskomponenten sollte ein Beschaffungsprozess eingehalten werden. Die Verträge mit dem Lieferanten sollten den festgestellten Sicherheitsanforderungen Rechnung tragen (siehe 5.20). Die Produkte und Dienste sollten vor dem Kauf anhand dieser Kriterien bewertet werden.

Die Überprüfung sollte in einer Testumgebung durchgeführt werden, die der angestrebten Produktionsumgebung so weit wie möglich entspricht, um sicherzustellen, dass das System keine Schwachstellen in der Betriebsumgebung der Organisation verursacht und dass die Überprüfungen zuverlässig sind (siehe 8.31).

Weitere Informationen

Es können mehrere Prüfumgebungen eingerichtet werden, die für verschiedene Arten von Prüfungen verwendet werden können (z. B. Funktions- und Leistungsprüfungen). Diese verschiedenen Umgebungen können virtuell sein, mit individuellen Konfigurationen, um eine Vielzahl von Betriebsumgebungen zu simulieren.

Auch das Prüfen und Überwachen von Prüfungsumgebungen, Werkzeugen und Technologien muss berücksichtigt werden, um wirksame Prüfungen sicherzustellen. Die gleichen Überlegungen gelten für die Überwachung der Überwachungssysteme, die in Entwicklungs-, Prüf- und Produktionsumgebungen eingesetzt werden. Je nach Empfindlichkeit der Systeme und Daten muss entschieden werden, wie viele Schichten von Meta-Tests sinnvoll sind.

8.30 Ausgegliederte Entwicklung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit	#Identifizieren	#System- und Netzwerksicherheit	#Governance_und_Ökosystem
#Detektiv	#Integrität #Verfügbarkeit	#Schützen #Erkennen	#Anwendungssicherheit #Sicherheit_in_Lieferantenbeziehungen	#Schutz

Maßnahme

Die Organisation sollte die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.

Zweck

Sicherstellen, dass die von der Organisation geforderten Maßnahmen zur Informationssicherheit in der ausgelagerten Systementwicklung umgesetzt werden.

Leitfaden

Wenn die Systementwicklung ausgelagert wird, sollte die Organisation die Anforderungen und Erwartungen kommunizieren und vereinbaren und kontinuierlich überwachen und überprüfen, ob die ausgelagerte Arbeit diese Erwartungen erfüllt. Die folgenden Punkte sollten über die gesamte externe Lieferkette der Organisation berücksichtigt werden:

- Lizenzierungsvereinbarungen, Eigentümerschaft an Programmcode und geistige Eigentumsrechte in Bezug auf die ausgelagerten Inhalte (siehe 5.32);
- vertragliche Anforderungen bezüglich des sicheren Entwurfs, der Programmierung und der Überprüfungspraxis (siehe 8.25 bis 8.29);
- Bereitstellung des Bedrohungsmodells zur Berücksichtigung durch externe Entwickler;
- Abnahmeprüfung bezüglich der Qualität und Genauigkeit der bereitgestellten Leistungen (siehe 8.29);
- Erbringung des Nachweises, dass ein annehmbares Mindestmaß an Sicherheit und Datenschutz gegeben ist (z. B. Vertrauenswürdigkeitsberichte);
- Nachweis, dass ausreichende Prüfungen durchgeführt wurden, um das Vorhandensein bössartiger Inhalte (sowohl absichtlich als auch unabsichtlich) bei der Zustellung auszuschließen;
- Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um das Vorhandensein bekannter Schwachstellen auszuschließen;

- h) Treuhandvereinbarungen für den Software-Quellcode (z. B. wenn der Lieferant seine Geschäftstätigkeit aufgibt);
- i) vertragliches Recht zur Überprüfung der Entwicklungsprozesse und Maßnahmen;
- j) Sicherheitsanforderungen für die Entwicklungsumgebung (siehe 8.31);
- k) unter Berücksichtigung der geltenden Rechtsvorschriften (z. B. über den Schutz personenbezogener Daten).

Weitere Informationen

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

8.31 Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Entwicklungs-, Prüf- und Produktionsumgebungen sollten getrennt und gesichert werden.

Zweck

Schutz der Produktionsumgebung und der Daten vor Beeinträchtigung durch Entwicklungs- und Prüftätigkeiten.

Leitfaden

Nachdem festgestellt wurde, wie stark Produktions-, Prüf- und Entwicklungsumgebungen zur Verhinderung von Problemen im Produktionsablauf voneinander getrennt werden müssen, sollte diese Trennung umgesetzt werden.

Die folgenden Punkte sollten dabei berücksichtigt werden:

- a) eine angemessene Trennung von Entwicklungs- und Produktionssystemen und deren Betrieb in unterschiedlichen Domänen (z. B. in getrennten virtuellen oder physischen Umgebungen);
- b) Festlegung, Dokumentation und Umsetzung von Regeln und Genehmigungen für den Einsatz von Software vom Entwicklungs- zum Produktionsstatus;
- c) Prüfung von Änderungen an Produktionssystemen und -anwendungen in einer Prüf- oder Staging-Umgebung, bevor sie auf Produktionssysteme angewendet werden (siehe 8.29);
- d) keine Prüfung in Produktionsumgebungen, es sei denn, die Umstände wurden festgelegt und genehmigt;

- e) Compiler, Editoren und andere Entwicklungswerkzeuge oder Dienstprogramme, die von Produktionssystemen aus nicht zugänglich sind, wenn sie nicht benötigt werden;
- f) die Anzeige geeigneter Umgebungskennzeichnungen in den Menüs, um das Fehlerrisiko zu verringern;
- g) kein Kopieren sensibler Informationen in die Entwicklungs- und Prüfsystemumgebung, es sei denn, dass entsprechende Maßnahmen für die Entwicklungs- und Prüfsysteme zur Verfügung stehen.

In jedem Fall sollten Entwicklungs- und Prüfumgebungen geschützt werden:

- a) Patchen und Aktualisieren aller Entwicklungs-, Integrations- und Prüfwerkzeuge (einschließlich Builders, Integrators, Compilers, Konfigurationssysteme und Bibliotheken);
- b) sichere Konfiguration von Systemen und Software;
- c) Kontrolle des Zugangs zu den Umgebungen;
- d) Überwachung von Änderungen an der Umgebung und darin gespeichertem Code;
- e) sichere Überwachung der Umgebungen;
- f) Erstellung von Sicherungskopien der Umgebungen.

Eine einzelne Person sollte nicht die Möglichkeit haben, ohne vorherige Prüfung und Genehmigung Änderungen sowohl in der Entwicklung als auch in der Produktion vorzunehmen. Dies kann z. B. durch eine Trennung der Zugangsrechte oder durch Regeln, die überwacht werden, erreicht werden. In Ausnahmesituationen sollten zusätzliche Maßnahmen wie eine detaillierte Protokollierung und Echtzeitüberwachung implementiert werden, um unberechtigte Änderungen zu erkennen und darauf zu reagieren.

Weitere Informationen

Ohne angemessene Maßnahmen und Verfahren können Entwickler und Prüfer, die Zugang zu Produktionssystemen haben, erhebliche Risiken eingehen (z. B. unerwünschte Änderung von Dateien oder der Systemumgebung, Systemausfälle, Ausführung von nicht genehmigtem und ungeprüftem Code in Produktionssystemen, Offenlegung vertraulicher Daten, Probleme mit der Datenintegrität und -verfügbarkeit). Die Aufrechterhaltung einer bekannten und stabilen Umgebung ist erforderlich, um sinnvolle Überprüfungen durchzuführen und einen unerwünschten Entwicklerzugriff auf die Produktionsumgebung zu verhindern.

Zu den Maßnahmen und Verfahren gehören sorgfältig ausgearbeitete Rollen in Verbindung mit der Umsetzung der Anforderungen an die Aufgabentrennung und die Einrichtung angemessener Überwachungsprozesse.

Entwickelnde und testende Beschäftigte stellen außerdem eine Bedrohung für die Vertraulichkeit der Produktionsdaten dar. Entwicklungs- und Prüftätigkeiten können zu unbeabsichtigten Veränderungen an der Software oder den Informationen führen, wenn sie in derselben Rechnerumgebung stattfinden. Eine Trennung der Entwicklungs-, Prüf- und Produktionsumgebung ist daher wünschenswert, um das Risiko unbeabsichtigter Veränderungen oder eines unbefugten Zugriffs auf die Produktionssoftware und die Geschäftsdaten zu verringern (zum Schutz der Prüfinformationen siehe 8.33).

In einigen Fällen kann die Unterscheidung zwischen Entwicklungs-, Prüf- und Produktionsumgebungen absichtlich verwischt werden, und die Prüfung kann in einer Entwicklungsumgebung oder durch kontrollierte Rollouts auf Live-Benutzer oder Server (z. B. eine kleine Gruppe von Pilotbenutzern) durchgeführt werden. In einigen Fällen können Produktprüfungen durch den Live-Einsatz des Produkts innerhalb der Organisation erfolgen. Darüber hinaus können zwei identische Produktionsumgebungen unterstützt werden, von denen jeweils nur eine in Betrieb ist, um die Ausfallzeiten bei Live-Bereitstellungen zu reduzieren.

Es sind unterstützende Prozesse für die Verwendung von Produktionsdaten in Entwicklungs- und Prüfumgebungen (siehe 8.33) erforderlich.

Organisationen können bei der Durchführung von Endbenutzerschulungen auch die in diesem Abschnitt für Schulungsumgebungen gegebenen Leitfäden berücksichtigen.

8.32 Änderungssteuerung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz

Maßnahme

Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen sollten Gegenstand von Änderungsmanagementverfahren sein.

Zweck

Zur Wahrung der Informationssicherheit bei der Durchführung von Änderungen.

Leitfaden

Die Einführung neuer Systeme und wesentlicher Änderungen an den bestehenden Systemen sollte nach vereinbarten Regeln und einem formellen Prozess erfolgen, welcher Dokumentation, Spezifikation, Prüfung, Qualitätskontrolle und begleitete Umsetzung umfasst. Es sollten Verantwortlichkeiten und Verfahren für die Handhabung existieren, um die zufriedenstellende Steuerung aller Änderungen sicherzustellen.

Verfahren zur Verwaltung von Systemänderungen sollten dokumentiert und durchgesetzt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Informationsverarbeitungseinrichtungen und Informationssystemen für den gesamten Lebenszyklus der Systementwicklung von den ersten Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen.

Wo immer dies möglich ist, sollten die Verfahren zur Verwaltung von Systemänderungen für IKT-Infrastruktur und Software integriert werden.

In den Verfahren zur Verwaltung von Systemänderungen sollten die folgenden Punkte berücksichtigt werden:

- Planung und Beurteilung der möglichen Auswirkungen von Änderungen unter Berücksichtigung aller Abhängigkeiten;
- Autorisierung von Änderungen;
- Mitteilung der Änderungen an die interessierten Parteien;
- Prüfungen und Abnahme der Prüfungen für die Änderungen (siehe 8.29);
- Umsetzung von Änderungen, einschließlich Einsatzplänen;
- Überlegungen zu Notfällen und Eventualitäten, einschließlich Ausweichverfahren;

- g) Führung von Aufzeichnungen über Änderungen, die alle oben genannten Punkte beinhalten;
- h) Sicherstellung, dass die Betriebsdokumentation (siehe 5.37) und die Benutzerverfahren nach Bedarf entsprechend geändert werden;
- i) Sicherstellung, dass die IKT-Kontinuitätspläne und die Reaktions- und Wiederherstellungsverfahren (siehe 5.30) bei Bedarf geändert werden, um angemessen zu bleiben.

Weitere Informationen

Die unzureichende Steuerung von Änderungen an Einrichtungen und Systemen zur Informationsverarbeitung ist eine häufige Ursache von System- oder Sicherheitsausfällen. Änderungen in der Produktionsumgebung, insbesondere bei der Übertragung von Software aus der Entwicklungs- in die Betriebsumgebung, können die Integrität und Verfügbarkeit von Anwendungen beeinträchtigen.

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

Es empfiehlt sich, die Überprüfung von IKT-Komponenten in einer Umgebung durchzuführen, die sowohl von der Produktions- als auch von der Entwicklungsumgebung getrennt ist (siehe 8.31). 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.

Zur Produktionsumgebung zählen Betriebssysteme, Datenbanken und Middleware-Plattformen. Die Maßnahmen sollten bei Anwendungs- und Infrastrukturänderungen angewendet werden.

8.33 Prüfinformationen

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität	#Schützen	#Informationsschutz	#Schutz

Maßnahme

Die Prüfinformationen sollten in geeigneter Weise ausgewählt, geschützt und verwaltet werden.

Zweck

Sicherstellung der Relevanz der Prüfung und des Schutzes der für die Prüfung verwendeten betrieblichen Informationen.

Leitfaden

Die Prüfinformationen sollten so ausgewählt werden, dass die Zuverlässigkeit der Prüfergebnisse und die Vertraulichkeit der relevanten betrieblichen Informationen sichergestellt sind. Sensible Informationen (einschließlich personenbezogener Daten) sollten nicht in die Entwicklungs- und Prüfumgebung kopiert werden (siehe 8.31).

Zum Schutz von Kopien betrieblicher Informationen, die zu Prüfzwecken verwendet werden, sollten die folgenden Leitlinien angewandt werden, unabhängig davon, ob die Prüfumgebung intern oder über einen Cloud-Dienst erstellt wird:

- a) Anwendung der gleichen Zugangssteuerungsverfahren für Prüfumgebungen wie für Betriebsumgebungen;
- b) jedes Mal eine separate Berechtigung, wenn Betriebsinformationen in eine Prüfumgebung kopiert werden;
- c) das Protokollieren des Kopierens und der Verwendung von Betriebsinformationen sollte so erfolgen, dass ein Prüfpfad existiert;
- d) Schutz sensibler Informationen durch Entfernung oder Maskierung (siehe 8.11), wenn sie für Prüfungen verwendet werden;
- e) ordnungsgemäßes Löschen (siehe 8.10) von Betriebsinformationen aus einer Prüfumgebung unmittelbar nach Abschluss der Prüfung, um eine unbefugte Nutzung von Prüfinformationen zu verhindern.

Die Prüfdaten sollten sicher gespeichert werden (um Manipulationen zu verhindern, die sonst zu ungültigen Ergebnissen führen können) und nur für Prüfzwecke verwendet werden.

Weitere Informationen

Die System- und Abnahmeprüfung kann erhebliche Mengen an Prüfinformationen erfordern, die den Betriebsinformationen möglichst ähnlich sein sollten.

8.34 Schutz der Informationssysteme während der Überwachungsprüfung

Maßnahmenart	Informationssicherheitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit #Informationsschutz	#Governance_und_Ökosystem #Schutz

Maßnahme

Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, sollten zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.

Zweck

Die Auswirkung von Audit- und anderen Vertrauenswürdigkeitstätigkeiten auf Systeme im Betrieb und Geschäftsprozesse ist minimiert.

Leitfaden

Die folgenden Richtlinien sollten beachtet werden:

- a) Abstimmung von Prüfungsanträgen für den Zugang zu Systemen und Daten mit dem zuständigen Management;
- b) Vereinbarung und Steuerung des Umfangs der technischen Prüfungen;

- c) Beschränkung der Audit-Prüfungen auf einen reinen Lesezugriff auf Software und Daten. Wenn kein Lesezugriff möglich ist, um die erforderlichen Informationen zu erhalten, sollte ein erfahrener Administrator, der über die erforderlichen Zugangsrechte verfügt, die Prüfung im Namen des Prüfers durchführen;
- d) wenn der Zugang gewährt wird, Festlegung und Überprüfung der Sicherheitsanforderungen (z. B. Virenschutz und Patches) der für den Zugang zu den Systemen verwendeten Geräte (z. B. Laptops oder Tablets), bevor der Zugang gewährt wird;
- e) nur für isolierte Kopien von Systemdateien einen anderen Zugang als nur Lesezugriff zuzulassen, sie nach Abschluss der Prüfung zu löschen oder sie angemessen zu schützen, wenn eine Verpflichtung zur Aufbewahrung solcher Dateien im Rahmen der Prüfungsunterlagen besteht;
- f) die Ermittlung und Genehmigung von Anträgen auf besondere oder zusätzliche Bearbeitung, wie z. B. die Durchführung von Audit-Tools;
- g) Durchführung von Auditprüfungen, die die Systemverfügbarkeit außerhalb der Geschäftszeiten beeinträchtigen können;
- h) Überwachung und Protokollierung aller Zugriffe zu Audit- und Prüfzwecken.

Weitere Informationen

Auditprüfungen und andere Vertrauenswürdigkeitsaktivitäten können auch auf Entwicklungs- und Prüfsystemen durchgeführt werden, wo sich solche Prüfungen beispielsweise auf die Integrität des Codes auswirken oder zur Offenlegung sensibler Informationen führen können, die sich in solchen Umgebungen befinden.

Normen-Download-Beuth-Heuteing Ktüm Lier-Wojtek PartGmbB-KdNr.7791402-ID.rc251_5DuGlsklPuDu08_xSFmunqyNFN210K056r-2023-07-12 11:26:52

Anhang A
(informativ)

Verwendung von Attributen

A.1 Allgemeines

Dieser Anhang enthält eine Tabelle zur Veranschaulichung der Verwendung von Attributen als Möglichkeit zur Erstellung verschiedener Ansichten der Maßnahmen. Die fünf Beispiele für Attribute sind (siehe 4.2):

- a) Maßnahmenarten (#Präventiv, #Detektiv, #Korrektiv);
- b) Eigenschaften der Informationssicherheit (#Vertraulichkeit, #Integrität, #Verfügbarkeit);
- c) Cybersecurity-Konzepte (#Identifizieren, #Schützen, #Erkennen, #Reagieren, #Wiederherstellen);
- d) Betriebsfähigkeit (#Governance, #Asset_Management, #Informationsschutz, #Sicherheit_der_Humanressourcen, #Physische_Sicherheit, #System- und Netzwerksicherheit, #Anwendungssicherheit, #Sichere_Konfiguration, #Identitäts- und Zugangsverwaltung, #Bedrohungs- und Schwachstellenmanagement, #Kontinuität, #Sicherheit_der_Lieferantenbeziehungen, #Recht_und_Compliance, #Informationssicherheits-Ereignismanagement und #Vertrauenswürdigkeit_in_Bezug_auf_die_Informationssicherheit);
- e) Sicherheitsdomänen (#Governance_und_Ökosystem, #Schutz, #Verteidigung, #Resilienz).

Tabelle A.1 enthält eine Matrix aller Maßnahmen in diesem Dokument mit den dazugehörigen Attributwerten.

Die Filterung oder Sortierung der Matrix kann mit Hilfe eines Tools wie einer einfachen Tabellenkalkulation oder einer Datenbank erfolgen, die weitere Informationen wie Kontrolltext, Leitfäden, organisations-spezifische Leitlinien oder Attribute enthalten kann (siehe A.2).

Tabelle A.1 — Matrix der Maßnahmen und Attributwerte

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.1	Informations- sicherheitsrichtlinien	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Öko- system #Resilienz
5.2	Informations- sicherheitsrollen und – verantwortlichkeiten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Öko- system #Schutz #Resilienz
5.3	Aufgabentrennung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Governance #Identitäts- und Zugangsverwaltung	#Governance_und_Öko- system
5.4	Verantwortlichkeiten der Leitung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Governance	#Governance_und_Öko- system
5.5	Kontakt mit Behörden	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung #Resilienz
5.6	Kontakt mit speziellen Interessensgruppen	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.7	Bedrohungsintelligenz	#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Erkennen #Reagieren	#Bedrohungs- und Schwachstellen- management	#Verteidigung #Resilienz
5.8	Informationssicherheit im Projektmanagement	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Governance	#Governance_und_Öko- system #Schutz
5.9	Inventar der Informationen und anderen damit verbun- denen Werten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Asset_Management	#Governance_und_Öko- system #Schutz
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbun- denen Werten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Governance_und_Öko- system #Schutz
5.11	Rückgabe von Werten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management	#Schutz
5.12	Klassifizierung von Information	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Informationsschutz	#Schutz #Verteidigung
5.13	Kennzeichnung von Information	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Informationsschutz	#Verteidigung #Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.14	Informations- übertragung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Schutz
5.15	Zugangssteuerung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
5.16	Identitätsmanagement	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
5.17	Informationen zur Authentifizierung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
5.18	Zugangsrechte	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
5.19	Informationssicherheit in Lieferanten- beziehungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lie- ferantenbeziehungen	#Governance_und_Öko- system #Schutz
5.20	Behandlung von Informationssicherheit in Lieferantenver- einbarungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lie- ferantenbeziehungen	#Governance_und_Öko- system #Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lie- ferantenbeziehungen	#Governance_und_Öko- system #Schutz
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferanten- dienstleistungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Sicherheit_in_Lie- ferantenbeziehungen #Vertrauenswür- digkeit_in_Bezug_auf_Inf- ormationssicherheit	#Governance_und_Öko- system #Schutz #Verteidigung
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_in_Lie- ferantenbeziehungen	#Governance_und_Öko- system #Schutz
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheits- vorfällen	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Governance #Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung
5.25	Beurteilung und Entscheidung über Informationssicherheits- ereignisse	#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung
5.26	Reaktion auf Informationssicherheits- vorfälle	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung
5.27	Erkenntnisse aus Informationssicherheits- vorfällen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.28	Sammeln von Beweismaterial	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung
5.29	Informationssicherheit bei Störungen	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren	#Aufrechterhaltung	#Schutz #Resilienz
5.30	IKT-Bereitschaft für Business Continuity	#Korrektiv	#Verfügbarkeit	#Reagieren	#Aufrechterhaltung	#Resilienz
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Recht_und_Compliance	#Governance_und_Öko- system #Schutz
5.32	Geistige Eigentumsrechte	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Recht_und_Compliance	#Governance_und_Öko- system
5.33	Schutz von Aufzeichnungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Recht_und_Compliance #Asset_Management #Informationsschutz	#Verteidigung
5.34	Datenschutz und Schutz personenbezogener Daten (pbd)	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Informationsschutz #Recht_und_Compliance	#Schutz
5.35	Unabhängige Überprüfung der Informationssicherheit	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Vertrauenswürdigkeit_in _Bezug_auf_Informations- sicherheit	#Governance_und_Öko- system

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Recht_und_Compliance #Vertrauenswürdigkeit_in _Bezug_auf_Informationss icherheit	#Governance_und_Öko- system
5.37	Dokumentierte Betriebsabläufe	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Wiederherstellen	#Asset_Management #Physische_Sicherheit #System- und Netzwerksicherheit #Anwendungssicherheit #Sichere_Konfiguration #Identitäts- und Zugangsverwaltung #Bedrohungs- und Schwachstellenmanageme nt #Aufrechterhaltung #Handhabung_von_Infor- mationssicherheitseig- nissen	#Governance_und_Öko- system #Schutz #Verteidigung
6.1	Sicherheitsüberprüfung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Human- ressourcen	#Governance_und_Öko- system
6.2	Beschäftigungs- und Vertragsbedingungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Human- ressourcen	#Governance_und_Öko- system

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
6.3	Informations- sicherheitsbe- wusstsein, -ausbildung und -schulung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Human- ressourcen	#Governance_und_Öko- system
6.4	Maßregelungsprozess	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren	#Sicherheit_der_Human- ressourcen	#Governance_und_Öko- system
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sicherheit_der_Human- ressourcen #Asset_Management	#Governance_und_Öko- system
6.6	Vertraulichkeits- oder Geheimhaltungsverein- barungen	#Präventiv	#Vertraulichkeit	#Schützen	#Sicherheit_der_Human- ressourcen #Informationsschutz #Lieferantenbeziehungen	#Governance_und_Öko- system
6.7	Telearbeit	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz #Physische_Sicherheit #System- und Netzwerksicherheit	#Schutz
6.8	Meldung von Informationssicherheits- ereignissen	#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
7.1	Physische Sicherheits- perimeter	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz
7.2	Physischer Zutritt	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Identitäts- und Zugangsverwaltung	#Schutz
7.3	Sichern von Büros, Räumen und Ein- richtungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz
7.4	Physische Sicherheits- überwachung	#Präventiv #Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Erkennen	#Physische_Sicherheit	#Schutz #Verteidigung
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz
7.6	Arbeiten in Sicherheits- bereichen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz
7.7	Aufgeräumte Arbeitsumgebung und Bildschirm Sperren	#Präventiv	#Vertraulichkeit	#Schützen	#Physische_Sicherheit	#Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz
7.9	Sicherheit von Werten außerhalb der Räum- lichkeiten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz
7.10	Speichermedien	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz
7.11	Versorgungs- einrichtungen	#Präventiv #Detektiv	#Integrität #Verfügbarkeit	#Schützen #Erkennen	#Physische_Sicherheit	#Schutz
7.12	Sicherheit der Verkabelung	#Präventiv	#Vertraulichkeit #Verfügbarkeit	#Schützen	#Physische_Sicherheit	#Schutz
7.13	Instandhaltung von Geräten und Betriebsmitteln	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz #Resilienz
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	#Präventiv	#Vertraulichkeit	#Schützen	#Physische_Sicherheit #Asset_Management	#Schutz
8.1	Endpunktgeräte des Benutzers	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
8.2	Privilegierte Zugangsrechte	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
8.3	Informationszugangs- beschränkung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
8.4	Zugriff auf den Quellcode	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung #Anwendungssicherheit #Sichere_Konfiguration	#Schutz
8.5	Sichere Authenti- fizierung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Identitäts- und Zugangsverwaltung	#Schutz
8.6	Kapazitätssteuerung	#Präventiv #Detektiv	#Integrität #Verfügbarkeit	#Identifizieren #Schützen #Erkennen	#Aufrechterhaltung	#Governance_und_Öko- system #Schutz
8.7	Schutz gegen Schadsoftware	#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Erkennen	#System- und Netzwerksicherheit #Informationsschutz	#Schutz #Verteidigung
8.8	Handhabung von technischen Schwachstellen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Bedrohungs- und Schwachstellenmanageme- nt	#Governance_und_Öko- system #Schutz #Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
8.9	Konfigurations- management	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration	#Schutz
8.10	Löschung von Informationen	#Präventiv	#Vertraulichkeit	#Schützen	#Informationsschutz #Recht_und_Compliance	#Schutz
8.11	Datenmaskierung	#Präventiv	#Vertraulichkeit	#Schützen	#Informationsschutz	#Schutz
8.12	Verhinderung von Datenlecks	#Präventiv #Detektiv	#Vertraulichkeit	#Schützen #Erkennen	#Informationsschutz	#Schutz #Verteidigung
8.13	Sicherung von Information	#Korrektiv	#Integrität #Verfügbarkeit	#Wiederherstellen	#Aufrechterhaltung	#Schutz
8.14	Redundanz von informations- verarbeitenden Einrichtungen	#Präventiv	#Verfügbarkeit	#Schützen	#Aufrechterhaltung #Asset_Management	#Schutz #Resilienz
8.15	Protokollierung	#Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Schutz #Verteidigung
8.16	Überwachung von Aktivitäten	#Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Verteidigung
8.17	Uhrensynchronisation	#Detektiv	#Integrität	#Schützen #Erkennen	#Handhabung_von_Infor- mationssicherheitsereig- nissen	#Schutz #Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
8.18	Gebrauch von Hilfs- programmen mit privilegierten Rechten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit #Sichere_Konfiguration #Anwendungssicherheit	#Schutz
8.19	Installation von Software auf Systemen im Betrieb	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration #Anwendungssicherheit	#Schutz
8.20	Netzwerksicherheit	#Präventiv #Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Erkennen	#System- und Netzwerksicherheit	#Schutz
8.21	Sicherheit von Netzwerkdiensten	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz
8.22	Trennung von Netzwerken	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz
8.23	Webfilterung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit	#Schutz
8.24	Verwendung von Kryptographie	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Sichere_Konfiguration	#Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
8.25	Lebenszyklus einer sicheren Entwicklung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz
8.26	Anforderungen an die Anwendungssicherheit	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz #Verteidigung
8.27	Sichere System- architektur und technische Grundsätze	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz
8.28	Sicheres Coding	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz
8.29	Sicherheitsprüfung in Entwicklung und Abnahme	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Anwendungssicherheit #Vertrauenswürdigkeit_in _Bezug_auf_Informations- sicherheit #System- und Netzwerksicherheit	#Schutz
8.30	Ausgegliederte Entwicklung	#Präventiv #Detektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen #Erkennen	#System- und Netzwerksicherheit #Anwendungssicherheit #Sicherheit_in_Lieferan- tenbeziehungen	#Governance_und_Öko- system #Schutz

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
8.31	Trennung von Entwicklungs-, Prüf- und Produktions- umgebungen	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz
8.32	Änderungssteuerung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Anwendungssicherheit #System- und Netzwerksicherheit	#Schutz
8.33	Informationen zur Prüfung	#Präventiv	#Vertraulichkeit#Inte- grität	#Schützen	#Informationsschutz	#Schutz
8.34	Schutz der Informations- systeme während der Überwachungsprüfung	#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#System- und Netzwerksicherheit #Informationsschutz	#Governance_und_Öko- system #Schutz

Tabelle A.2 zeigt ein Beispiel für die Erstellung einer Ansicht durch Filterung nach einem bestimmten Attributwert, in diesem Fall #Korrektiv.

Tabelle A.2 — Ansicht der #Korrektivmaßnahmen

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.5	Kontakt mit Behörden	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung #Resilienz
5.6	Kontakt mit speziellen Interessensgruppen	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren #Wiederherstellen	#Governance	#Verteidigung
5.7	Bedrohungsintelligenz	#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Erkennen #Reagieren	#Bedrohungs- und Schwachstellenmanage- ment	#Verteidigung #Resilienz
5.24	Planung und Vorbereitung der Handhabung von Informa- tionssicherheits- vorfällen	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Governance #Handhabung_von_In- formationssicherheits- ereignissen	#Verteidigung
5.26	Reaktion auf Informationss- icherheitsvorfälle	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Reagieren #Wiederherstellen	#Handhabung_von_In- formationssicherheits- ereignissen	#Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
5.28	Sammeln von Beweismaterial	#Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_In- formationssicherheits- ereignissen	#Verteidigung
5.29	Informationssicherheit bei Störungen	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren	#Aufrechterhaltung	#Schutz #Resilienz
5.30	IKT-Bereitschaft für Business Continuity	#Korrektiv	#Verfügbarkeit	#Reagieren	#Aufrechterhaltung	#Resilienz
5.35	Unabhängige Überprüfung der Informationssicherheit	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Schützen	#Vertrauenswürdigkeit_ in_Bezug_auf_Informa- tionssicherheit	#Governance_und_Ök osystem
5.37	Dokumentierte Betriebsabläufe	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Wiederherstellen	#Asset_Management #Physische_Sicherheit #System- und Netzwerksicherheit #Anwendungssicherheit #Sichere_Konfiguration #Identitäts- und Zugangsverwaltung #Bedrohungs- und Schwachstellenmanage ment #Aufrechterhaltung	#Governance_und_Ök osystem #Schutz #Verteidigung

ISO/IEC 27002 Maßnahmen- kennung	Maßnahmenname	Maßnahmenart	Informations- sicherheits- eigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
					#Handhabung_von_In- formationssicherheits- ereignissen	
6.4	Maßregelungsprozess	#Präventiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Reagieren	#Sicherheit_der_Human ressourcen	#Governance_und_Ök osystem
8.7	Schutz gegen Schadsoftware	#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen #Erkennen	#System- und Netzwerksicherheit #Informationsschutz	#Schutz #Verteidigung
8.13	Sicherung von Information	#Korrektiv	#Integrität #Verfügbarkeit	#Wiederherstellen	#Aufrechterhaltung	#Schutz
8.16	Überwachung von Aktivitäten	#Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Erkennen #Reagieren	#Handhabung_von_In- formationssicherheits- ereignissen	#Verteidigung

A.2 Organisatorische Sichten

Da Attribute verwendet werden, um unterschiedliche Sichten auf Maßnahmen zu erstellen, können Organisationen die in diesem Dokument vorgeschlagenen Beispiele für Attribute verwerfen und ihre eigenen Attribute mit unterschiedlichen Werten erstellen, um spezifische Anforderungen in der Organisation zu erfüllen. Darüber hinaus können die den einzelnen Attributen zugewiesenen Werte von Organisation zu Organisation unterschiedlich sein, da die Organisationen unterschiedliche Ansichten über die Verwendung oder Anwendbarkeit der Kontrollmaßnahmen oder der mit dem Attribut verbundenen Werte haben können (wenn die Werte für den Kontext der Organisation spezifisch sind). Der erste Schritt besteht darin zu verstehen, warum ein organisationsspezifisches Attribut wünschenswert ist. Wenn eine Organisation beispielsweise ihre Risikobehandlungspläne [siehe ISO/IEC 27001:2013, 6.1.3 e)] auf der Grundlage von Ereignissen erstellt hat, kann sie jeder Maßnahme in diesem Dokument ein Attribut für ein Risikoszenario zuordnen.

Der Vorteil eines solchen Attributs besteht darin, dass es den Prozess der Erfüllung der ISO/IEC 27001-Anforderung in Bezug auf die Risikobehandlung beschleunigt, d. h. den Vergleich der durch den Prozess der Risikobehandlung ermittelten Maßnahmen (die als „notwendige“ Maßnahmen bezeichnet werden) mit denen in ISO/IEC 27001:2013, Anhang A (die in diesem Dokument enthalten sind), um sicherzustellen, dass keine notwendige Maßnahme übersehen wurde.

Sobald der Zweck und der Nutzen bekannt sind, besteht der nächste Schritt darin, die Attributwerte zu bestimmen. Die Organisation könnte zum Beispiel 9 Ereignisse identifizieren:

- 1) Verlust oder Diebstahl des Mobilgeräts;
- 2) Verlust oder Diebstahl aus den Räumlichkeiten der Organisation;
- 3) höhere Gewalt, Vandalismus und Terrorismus;
- 4) Ausfall von Software, Hardware, Strom, Internet und Kommunikation;
- 5) Betrug;
- 6) Hacking;
- 7) Offenlegung;
- 8) Verstoß gegen das Gesetz;
- 9) Social Engineering.

Der zweite Schritt kann daher durch die Zuweisung von Identifikatoren für jedes Ereignis (z. B. E1, E2, ..., E9) durchgeführt werden.

Der dritte Schritt besteht darin, die Steuerungskennungen und -namen aus diesem Dokument in eine Tabellenkalkulation oder Datenbank zu kopieren und die Attributwerte den einzelnen Steuerungen zuzuordnen, wobei zu beachten ist, dass jede Steuerungs mehr als einen Attributwert haben kann.

Der letzte Schritt besteht darin, die Tabelle zu sortieren oder die Datenbank abzufragen, um die gewünschten Informationen zu extrahieren.

Weitere Beispiele für Organisationsattribute (und mögliche Werte) sind:

- a) Reifegrad (Werte aus der Normenreihe ISO/IEC 33000 oder andere Reifegradmodelle);
- b) Umsetzungsstatus (zu tun, in Arbeit, teilweise umgesetzt, vollständig umgesetzt);
- c) Priorität (1, 2, 3, usw.);
- d) beteiligte organisatorische Bereiche (Sicherheit, IKT, Humanressourcen, Topmanagement usw.);
- e) Ereignisse;
- f) betroffene Werte;
- e) Build und Run, um die in den verschiedenen Phasen des Lebenszyklus der Dienstleistung verwendeten Maßnahmen zu unterscheiden;
- g) andere Rahmenwerke, mit denen die Organisation arbeitet oder von denen sie möglicherweise abweicht.

Anhang B (informativ)

Übereinstimmung von ISO/IEC 27002:2022 (dieses Dokument) mit ISO/IEC 27002:2013

Der Zweck dieses Anhangs ist es, die Abwärtskompatibilität mit ISO/IEC 27002:2013 für Organisationen zu gewährleisten, die derzeit diese Norm verwenden und nun auf diese Ausgabe umsteigen möchten.

Tabelle B.1 zeigt die Übereinstimmung der in Abschnitt 5 bis Abschnitt 8 spezifizierten Maßnahmen mit denen in ISO/IEC 27002:2013.

Tabelle B.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/IEC 27002:2013

ISO/IEC 27002:2022 Maßnahmen- kennung	ISO/IEC 27002:2013 Maßnahmen- kennung	Maßnahmenname
5.1	05.1.1, 05.1.2	Informationssicherheitsrichtlinien
5.2	06.1.1	Informationssicherheitsrollen und -verantwortlichkeiten
5.3	06.1.2	Aufgabentrennung
5.4	07.2.1	Verantwortlichkeiten der Leitung
5.5	06.1.3	Kontakt mit Behörden
5.6	06.1.4	Kontakt mit speziellen Interessensgruppen
5.7	Neu	Bedrohungsentelligenz
5.8	06.1.5, 14.1.1	Informationssicherheit im Projektmanagement
5.9	08.1.1, 08.1.2	Inventar der Informationen und anderen damit verbundenen Werten
5.10	08.1.3, 08.2.3	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
5.11	08.1.4	Rückgabe von Werten
5.12	08.2.1	Klassifizierung von Information
5.13	08.2.2	Kennzeichnung von Information
5.14	13.2.1, 13.2.2, 13.2.3	Informationsübertragung
5.15	09.1.1, 09.1.2	Zugangssteuerung
5.16	09.2.1	Identitätsmanagement
5.17	09.2.4, 09.3.1, 09.4.3	Informationen zur Authentifizierung
5.18	09.2.2, 09.2.5, 09.2.6	Zugangsrechte
5.19	15.1.1	Informationssicherheit in Lieferantenbeziehungen
5.20	15.1.2	Behandlung von Informationssicherheit in Lieferantenvereinbarungen
5.21	15.1.3	Umgang mit der Informationssicherheit in der IKT-Lieferkette
5.22	15.2.1, 15.2.2	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
5.23	Neu	Informationssicherheit für die Nutzung von Cloud-Diensten
5.24	16.1.1	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

ISO/IEC 27002:2022 Maßnahmen- kennung	ISO/IEC 27002:2013 Maßnahmen- kennung	Maßnahmenname
5.25	16.1.4	Beurteilung und Entscheidung über Informationssicherheitsereignisse
5.26	16.1.5	Reaktion auf Informationssicherheitsvorfälle
5.27	16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen
5.28	16.1.7	Sammeln von Beweismaterial
5.29	17.1.1, 17.1.2, 17.1.3	Informationssicherheit bei Störungen
5.30	Neu	IKT-Bereitschaft für Business Continuity
5.31	18.1.1, 18.1.5	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
5.32	18.1.2	Geistige Eigentumsrechte
5.33	18.1.3	Schutz von Aufzeichnungen
5.34	18.1.4	Datenschutz und Schutz personenbezogener Daten (pbD)
5.35	18.2.1	Unabhängige Überprüfung der Informationssicherheit
5.36	18.2.2, 18.2.3	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
5.37	12.1.1	Dokumentierte Betriebsabläufe
6.1	07.1.1	Sicherheitsüberprüfung
6.2	07.1.2	Beschäftigungs- und Vertragsbedingungen
6.3	07.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung
6.4	07.2.3	Maßregelungsprozess
6.5	07.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
6.6	13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen
6.7	06.2.2	Telearbeit
6.8	16.1.2, 16.1.3	Meldung von Informationssicherheitsereignissen
7.1	11.1.1	Physische Sicherheitsperimeter
7.2	11.1.2, 11.1.6	Physischer Zutritt
7.3	11.1.3	Sichern von Büros, Räumen und Einrichtungen
7.4	Neu	Physische Sicherheitsüberwachung
7.5	11.1.4	Schutz vor physischen und umweltbedingten Bedrohungen
7.6	11.1.5	Arbeiten in Sicherheitsbereichen
7.7	11.2.9	Aufgeräumte Arbeitsumgebung und Bildschirmsperren
7.8	11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln
7.9	11.2.6	Sicherheit von Werten außerhalb der Räumlichkeiten
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Speichermedien
7.11	11.2.2	Versorgungseinrichtungen
7.12	11.2.3	Sicherheit der Verkabelung
7.13	11.2.4	Instandhaltung von Geräten und Betriebsmitteln
7.14	11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
8.1	06.2.1, 11.2.8	Endpunktgeräte des Benutzers
8.2	09.2.3	Privilegierte Zugangsrechte
8.3	09.4.1	Informationszugangsbeschränkung

ISO/IEC 27002:2022 Maßnahmen- kennung	ISO/IEC 27002:2013 Maßnahmen- kennung	Maßnahmenname
8.4	09.4.5	Zugriff auf den Quellcode
8.5	09.4.2	Sichere Authentifizierung
8.6	12.1.3	Kapazitätssteuerung
8.7	12.2.1	Schutz gegen Schadsoftware
8.8	12.6.1, 18.2.3	Handhabung von technischen Schwachstellen
8.9	Neu	Konfigurationsmanagement
8.10	Neu	Löschung von Informationen
8.11	Neu	Datenmaskierung
8.12	Neu	Verhinderung von Datenlecks
8.13	12.3.1	Sicherung von Information
8.14	17.2.1	Redundanz von informationsverarbeitenden Einrichtungen
8.15	12.4.1, 12.4.2, 12.4.3	Protokollierung
8.16	Neu	Überwachungstätigkeiten
8.17	12.4.4	Uhrensynchronisation
8.18	09.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten
8.19	12.5.1, 12.6.2	Installation von Software auf Systemen im Betrieb
8.20	13.1.1	Netzwerksicherheit
8.21	13.1.2	Sicherheit von Netzwerkdiensten
8.22	13.1.3	Trennung von Netzwerken
8.23	Neu	Webfilterung
8.24	10.1.1, 10.1.2	Verwendung von Kryptographie
8.25	14.2.1	Lebenszyklus einer sicheren Entwicklung
8.26	14.1.2, 14.1.3	Anforderungen an die Anwendungssicherheit
8.27	14.2.5	Sichere Systemarchitektur und technische Grundsätze
8.28	Neu	Sicheres Coding
8.29	14.2.8, 14.2.9	Sicherheitsprüfung bei Entwicklung und Abnahme
8.30	14.2.7	Ausgegliederte Entwicklung
8.31	12.1.4, 14.2.6	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Änderungssteuerung
8.33	14.3.1	Prüfinformationen
8.34	12.7.1	Schutz der Informationssysteme während der Überwachungsprüfung

Tabelle B.2 zeigt die Übereinstimmung der in ISO/IEC 27002:2013 spezifizierten Maßnahmen mit denen in diesem Dokument.

Tabelle B.2 — Übereinstimmung zwischen Maßnahmen in ISO/IEC 27002:2013 und Maßnahmen in diesem Dokument

ISO/IEC 27002:2013 Maßnahmen- kennung	ISO/IEC 27002:2022 Maßnahmen- kennung	Steuerungsbezeichnung nach ISO/IEC 27002:2013
5		Informationssicherheitsrichtlinien
5.1		Vorgaben der Leitung für Informationssicherheit
5.1.1	5.1	Informationssicherheitsrichtlinien
5.1.2	5.1	Überprüfung der Informationssicherheitsrichtlinien
6		Organisation der Informationssicherheit
6.1		Interne Organisation
6.1.1	5.2	Informationssicherheitsrollen und -verantwortlichkeiten
6.1.2	5.3	Aufgabentrennung
6.1.3	5.5	Kontakt mit Behörden
6.1.4	5.6	Kontakt mit speziellen Interessensgruppen
6.1.5	5.8	Informationssicherheit im Projektmanagement
6.2		Mobilgeräte und Telearbeit
6.2.1	8.1	Richtlinie zu Mobilgeräten
6.2.2	6.7	Telearbeit
7		Personalsicherheit
7.1		Vor der Beschäftigung
7.1.1	6.1	Sicherheitsüberprüfung
7.1.2	6.2	Beschäftigungs- und Vertragsbedingungen
7.2		Während der Beschäftigung
7.2.1	5.4	Verantwortlichkeiten der Leitung
7.2.2	6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung
7.2.3	6.4	Maßregelungsprozess
7.3		Beendigung und Änderung der Beschäftigung
7.3.1	6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
8		Verwaltung der Werte
8.1		Verantwortlichkeit für Werte
8.1.1	5.9	Inventarisierung der Werte
8.1.2	5.9	Zuständigkeit für Werte
8.1.3	5.10	Zulässiger Gebrauch von Werten
8.1.4	5.11	Rückgabe von Werten
8.2		Informationsklassifizierung
8.2.1	5.12	Klassifizierung von Information
8.2.2	5.13	Kennzeichnung von Information
8.2.3	5.10	Handhabung von Werten
8.3		Handhabung von Datenträgern
8.3.1	7.10	Handhabung von Wechseldatenträgern
8.3.2	7.10	Entsorgung von Datenträgern
8.3.3	7.10	Transport von Datenträgern

ISO/IEC 27002:2013 Maßnahmen- kennung	ISO/IEC 27002:2022 Maßnahmen- kennung	Steuerungsbezeichnung nach ISO/IEC 27002:2013
9		Zugangssteuerung
9.1		Geschäftsanforderungen an die Zugangsteuerung
9.1.1	5.15	Zugangssteuerungsrichtlinie
9.1.2	5.15	Zugang zu Netzwerken und Netzwerkdiensten
9.2		Benutzerzugangsverwaltung
9.2.1	5.16	Registrierung und Deregistrierung von Benutzern
9.2.2	5.18	Zuteilung von Benutzerzugängen
9.2.3	8.2	Verwaltung privilegierter Zugangsrechte
9.2.4	5.17	Verwaltung geheimer Authentisierungsinformation von Benutzern
9.2.5	5.18	Überprüfung von Benutzerzugangsrechten
9.2.6	5.18	Entzug oder Anpassung von Zugangsrechten
9.3		Benutzerverantwortlichkeiten
9.3.1	5.17	Gebrauch geheimer Authentisierungsinformation
9.4		Zugangssteuerung für Systeme und Anwendungen
9.4.1	8.3	Informationszugangsbeschränkung
9.4.2	8.5	Sichere Anmeldeverfahren
9.4.3	5.17	System zur Verwaltung von Kennwörtern
9.4.4	8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten
9.4.5	8.4	Zugangssteuerung für Quellcode von Programmen
10		Kryptographie
10.1		Kryptographische Maßnahmen
10.1.1	8.24	Richtlinie zum Gebrauch von kryptographischen Maßnahmen
10.1.2	8.24	Schlüsselverwaltung
11		Physische und umgebungsbezogene Sicherheit
11.1		Sicherheitsbereiche
11.1.1	7.1	Physische Sicherheitsperimeter
11.1.2	7.2	Physische Zutrittssteuerung
11.1.3	7.3	Sichern von Büros, Räumen und Einrichtungen
11.1.4	7.5	Schutz vor externen und umweltbedingten Bedrohungen
11.1.5	7.6	Arbeiten in Sicherheitsbereichen
11.1.6	7.2	Anlieferungs- und Ladebereiche
11.2		Geräte und Betriebsmittel
11.2.1	7.8	Platzierung und Schutz von Geräten und Betriebsmitteln
11.2.2	7.11	Versorgungseinrichtungen
11.2.3	7.12	Sicherheit der Verkabelung
11.2.4	7.13	Instandhaltung von Geräten und Betriebsmitteln
11.2.5	7.10	Entfernen von Werten
11.2.6	7.9	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten
11.2.7	7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

ISO/IEC 27002:2013 Maßnahmen- kennung	ISO/IEC 27002:2022 Maßnahmen- kennung	Steuerungsbezeichnung nach ISO/IEC 27002:2013
11.2.8	8.1	Unbeaufsichtigte Benutzergeräte
11.2.9	7.7	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren
12		Betriebssicherheit
12.1		Betriebsabläufe und -verantwortlichkeiten
12.1.1	5.37	Dokumentierte Betriebsabläufe
12.1.2	8.32	Änderungssteuerung
12.1.3	8.6	Kapazitätssteuerung
12.1.4	8.31	Trennung von Entwicklungs-, Test- und Betriebsumgebungen
12.2		Schutz vor Schadsoftware
12.2.1	8.7	Maßnahmen gegen Schadsoftware
12.3		Datensicherung
12.3.1	8.13	Sicherung von Information
12.4		Protokollierung und Überwachung
12.4.1	8.15	Ereignisprotokollierung
12.4.2	8.15	Schutz der Protokollinformation
12.4.3	8.15	Administratoren- und Bedienerprotokolle
12.4.4	8.17	Uhrensynchronisation
12.5		Steuerung von Software im Betrieb
12.5.1	8.19	Installation von Software auf Systemen im Betrieb
12.6		Handhabung technischer Schwachstellen
12.6.1	8.8	Handhabung von technischen Schwachstellen
12.6.2	8.19	Einschränkungen von Softwareinstallation
12.7		Audits von Informationssystemen
12.7.1	8.34	Maßnahmen für Audits von Informationssystemen
13		Kommunikationssicherheit
13.1		Einrichtungen für das Netzwerksicherheitsmanagement
13.1.1	8.20	Netzwerksteuerungsmaßnahmen
13.1.2	8.21	Sicherheit von Netzwerkdiensten
13.1.3	8.22	Trennung in Netzwerken
13.2		Informationsübertragung
13.2.1	5.14	Richtlinien und Verfahren für die Informationsübertragung
13.2.2	5.14	Vereinbarungen zur Informationsübertragung
13.2.3	5.14	Elektronische Nachrichtenübermittlung
13.2.4	6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen
14		Anschaffung, Entwicklung und Instandhaltung von Systemen
14.1		Sicherheitsanforderungen an Informationssysteme
14.1.1	5.8	Analyse und Spezifikation von Informationssicherheitsanforderungen
14.1.2	8.26	Sicherung von Anwendungsdiensten in öffentlichen Netzen
14.1.3	8.26	Schutz der Transaktionen bei Anwendungsdiensten
14.2		Sicherheit in Entwicklungs- und Unterstützungsprozessen

ISO/IEC 27002:2013 Maßnahmen- kennung	ISO/IEC 27002:2022 Maßnahmen- kennung	Steuerungsbezeichnung nach ISO/IEC 27002:2013
14.2.1	8.25	Richtlinie für sichere Entwicklung
14.2.2	8.32	Verfahren zur Verwaltung von Systemänderungen
14.2.3	8.32	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform
14.2.4	8.32	Beschränkung von Änderungen an Softwarepaketen
14.2.5	8.27	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme
14.2.6	8.31	Sichere Entwicklungsumgebung
14.2.7	8.30	Ausgegliederte Entwicklung
14.2.8	8.29	Testen der Systemsicherheit
14.2.9	8.29	Systemabnahmetest
14.3		Testdaten
14.3.1	8.33	Schutz von Testdaten
15		Lieferantenbeziehungen
15.1		Informationssicherheit in Lieferantenbeziehungen
15.1.1	5.19	Informationssicherheitsrichtlinie für Lieferantenbeziehungen
15.1.2	5.20	Behandlung von Sicherheit in Lieferantenvereinbarungen
15.1.3	5.21	Lieferkette für Informations- und Kommunikationstechnologie
15.2		Steuerung der Dienstleistungserbringung von Lieferanten
15.2.1	5.22	Überwachung und Überprüfung von Lieferantendienstleistungen
15.2.2	5.22	Handhabung der Änderungen von Lieferantendienstleistungen
16		Handhabung von Informationssicherheitsvorfällen
16.1		Handhabung von Informationssicherheitsvorfällen und -verbesserungen
16.1.1	5.24	Verantwortlichkeiten und Verfahren
16.1.2	6.8	Meldung von Informationssicherheitsereignissen
16.1.3	6.8	Meldung von Schwächen in der Informationssicherheit
16.1.4	5.25	Beurteilung von und Entscheidung über Informationssicherheitsereignisse
16.1.5	5.26	Reaktion auf Informationssicherheitsvorfälle
16.1.6	5.27	Erkenntnisse aus Informationssicherheitsvorfällen
16.1.7	5.28	Sammeln von Beweismaterial
17		Informationssicherheitsaspekte beim Business Continuity Management
17.1		Aufrechterhalten der Informationssicherheit
17.1.1	5.29	Planung zur Aufrechterhaltung der Informationssicherheit
17.1.2	5.29	Umsetzung der Aufrechterhaltung der Informationssicherheit
17.1.3	5.29	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit
17.2		Redundanzen
17.2.1	8.14	Verfügbarkeit von informationsverarbeitenden Einrichtungen
18		Compliance
18.1		Einhaltung gesetzlicher und vertraglicher Anforderungen

ISO/IEC 27002:2013 Maßnahmen- kennung	ISO/IEC 27002:2022 Maßnahmen- kennung	Steuerungsbezeichnung nach ISO/IEC 27002:2013
18.1.1	5.31	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen
18.1.2	5.32	Geistige Eigentumsrechte
18.1.3	5.33	Schutz von Aufzeichnungen
18.1.4	5.34	Privatsphäre und Schutz von personenbezogener Information
18.1.5	5.31	Regelungen bezüglich kryptographischer Maßnahmen
18.2		Überprüfungen der Informationssicherheit
18.2.1	5.35	Unabhängige Überprüfung der Informationssicherheit
18.2.2	5.36	Einhaltung von Sicherheitsrichtlinien und -standards
18.2.3	5.36, 8.8	Überprüfung der Einhaltung von technischen Vorgaben

Literaturhinweise

- [1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO 55001, *Asset management — Management systems — Requirements*
- [3] ISO/IEC 11770 (alle Teile), *Information security — Key management*
- [4] ISO/IEC 15408 (alle Teile), *Information technology — Security techniques — Evaluation criteria for IT security*
- [5] ISO 15489 (alle Teile), *Information and documentation — Records management*
- [6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
- [7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
- [8] ISO/IEC 19086 (alle Teile), *Cloud computing — Service level agreement (SLA) framework*
- [9] ISO/IEC 19770 (alle Teile), *Information technology — IT asset management*
- [10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- [11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
- [12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
- [13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
- [14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
- [15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
- [16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
- [17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
- [18] ISO/IEC TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
- [19] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
- [20] ISO/IEC 24760 (alle Teile), *IT Security and Privacy — A framework for identity management*
- [21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
- [22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

- [23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
- [24] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*
- [25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*
- [26] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
- [27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
- [30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [31] ISO/IEC 27033 (alle Teile), *Information technology — Security techniques — Network security*
- [32] ISO/IEC 27034 (alle Teile), *Information technology — Application security*
- [33] ISO/IEC 27035 (alle Teile), *Information technology — Security techniques — Information security incident management*
- [34] ISO/IEC 27036 (alle Teile), *Information technology — Security techniques — Information security for supplier relationships*
- [35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [37] ISO/IEC 27050 (alle Teile), *Information technology — Electronic discovery*
- [38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
- [39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
- [40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
- [41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
- [42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
- [43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*

- [44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
- [45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
- [46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
- [47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
- [48] ISO 31000:2018, *Risk management — Guidelines*
- [49] IEC 31010, *Risk management — Risk assessment techniques*
- [50] ISO/IEC 22123 (alle Teile), *Information technology — Cloud computing*
- [51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*
- [52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at <https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/>
- [53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076
- [54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-37r2>
- [55] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- [56] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at <https://github.com/OWASP/DevGuide>
- [57] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-63b>
- [58] OASIS. Structured Threat Information Expression. Available at <https://www.oasis-open.org/standards#stix2.0>
- [59] OASIS. Trusted Automated Exchange of Indicator Information. Available at <https://www.oasis-open.org/standards#taxii2.0>

Contents

Page

Foreword.....	vi
Introduction.....	vii
1 Scope.....	1
2 Normative references.....	1
3 Terms, definitions and abbreviated terms.....	1
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	6
4 Structure of this document.....	7
4.1 Clauses.....	7
4.2 Themes and attributes.....	8
4.3 Control layout.....	9
5 Organizational controls.....	9
5.1 Policies for information security.....	9
5.2 Information security roles and responsibilities.....	11
5.3 Segregation of duties.....	12
5.4 Management responsibilities.....	13
5.5 Contact with authorities.....	14
5.6 Contact with special interest groups.....	15
5.7 Threat intelligence.....	15
5.8 Information security in project management.....	17
5.9 Inventory of information and other associated assets.....	18
5.10 Acceptable use of information and other associated assets.....	20
5.11 Return of assets.....	21
5.12 Classification of information.....	22
5.13 Labelling of information.....	23
5.14 Information transfer.....	24
5.15 Access control.....	27
5.16 Identity management.....	29
5.17 Authentication information.....	30
5.18 Access rights.....	32
5.19 Information security in supplier relationships.....	33
5.20 Addressing information security within supplier agreements.....	35
5.21 Managing information security in the ICT supply chain.....	37
5.22 Monitoring, review and change management of supplier services.....	39
5.23 Information security for use of cloud services.....	41
5.24 Information security incident management planning and preparation.....	43
5.25 Assessment and decision on information security events.....	45
5.26 Response to information security incidents.....	45
5.27 Learning from information security incidents.....	46
5.28 Collection of evidence.....	47
5.29 Information security during disruption.....	48
5.30 ICT readiness for business continuity.....	48
5.31 Legal, statutory, regulatory and contractual requirements.....	50
5.32 Intellectual property rights.....	51
5.33 Protection of records.....	53
5.34 Privacy and protection of PII.....	54
5.35 Independent review of information security.....	55
5.36 Compliance with policies, rules and standards for information security.....	56
5.37 Documented operating procedures.....	57
6 People controls.....	58
6.1 Screening.....	58
6.2 Terms and conditions of employment.....	59

6.3	Information security awareness, education and training.....	60
6.4	Disciplinary process.....	62
6.5	Responsibilities after termination or change of employment.....	63
6.6	Confidentiality or non-disclosure agreements.....	63
6.7	Remote working.....	65
6.8	Information security event reporting.....	66
7	Physical controls.....	67
7.1	Physical security perimeters.....	67
7.2	Physical entry.....	68
7.3	Securing offices, rooms and facilities.....	70
7.4	Physical security monitoring.....	70
7.5	Protecting against physical and environmental threats.....	71
7.6	Working in secure areas.....	72
7.7	Clear desk and clear screen.....	73
7.8	Equipment siting and protection.....	74
7.9	Security of assets off-premises.....	75
7.10	Storage media.....	76
7.11	Supporting utilities.....	77
7.12	Cabling security.....	78
7.13	Equipment maintenance.....	79
7.14	Secure disposal or re-use of equipment.....	80
8	Technological controls.....	81
8.1	User endpoint devices.....	81
8.2	Privileged access rights.....	83
8.3	Information access restriction.....	84
8.4	Access to source code.....	86
8.5	Secure authentication.....	87
8.6	Capacity management.....	89
8.7	Protection against malware.....	90
8.8	Management of technical vulnerabilities.....	92
8.9	Configuration management.....	95
8.10	Information deletion.....	97
8.11	Data masking.....	98
8.12	Data leakage prevention.....	100
8.13	Information backup.....	101
8.14	Redundancy of information processing facilities.....	102
8.15	Logging.....	103
8.16	Monitoring activities.....	106
8.17	Clock synchronization.....	108
8.18	Use of privileged utility programs.....	109
8.19	Installation of software on operational systems.....	110
8.20	Networks security.....	111
8.21	Security of network services.....	112
8.22	Segregation of networks.....	113
8.23	Web filtering.....	114
8.24	Use of cryptography.....	115
8.25	Secure development life cycle.....	117
8.26	Application security requirements.....	118
8.27	Secure system architecture and engineering principles.....	120
8.28	Secure coding.....	122
8.29	Security testing in development and acceptance.....	124
8.30	Outsourced development.....	126
8.31	Separation of development, test and production environments.....	127
8.32	Change management.....	128
8.33	Test information.....	129
8.34	Protection of information systems during audit testing.....	130
	Annex A (informative) Using attributes.....	132

Annex B (informative) Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013 143

Bibliography 150

Normen-Download-Beuth-Heinking Kühn Lier-Wojtek PartGmbB-KdNr. 7791402-ID.rc25L5DuGlsklPuDu08_xSFmunqvNFV210K056r-2023-07-12 11:26:52

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

'This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27002:2013), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 27002:2013/Cor. 1:2014 and ISO/IEC 27002:2013/Cor. 2:2015.

The main changes are as follows:

- the title has been modified;
- the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;
- some controls have been merged, some deleted and several new controls have been introduced. The complete correspondence can be found in Annex B.

This corrected version of ISO/IEC 27002:2022 incorporates the following corrections:

- non-functioning hyperlinks throughout the document have been restored;
- in the introductory table in subclause 5.22 and in Table A.1 (row 5.22), "#information_security_assurance" has been moved from the column headed "Security domains" to the column headed "Operational capabilities".

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

- a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;
- b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;

- c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

- Entwurf -

Information security, cybersecurity and privacy protection — Information security controls

1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;
- b) for implementing information security controls based on internationally recognized best practices;
- c) for developing organization-specific information security management guidelines.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1.1

access control

means to ensure that physical and logical access to *assets* (3.1.2) is authorized and restricted based on business and information security requirements

3.1.2

asset

anything that has value to the organization

Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:

- the primary assets:
 - information;
 - business *processes* (3.1.27) and activities;
- the supporting assets (on which the primary assets rely) of all types, for example:
 - hardware;
 - software;
 - network;
 - *personnel* (3.1.20);

- site;
- organization's structure.

3.1.3

attack

successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an *asset* (3.1.2) or any attempt to expose, steal, or make unauthorized use of an *asset* (3.1.2)

3.1.4

authentication

provision of assurance that a claimed characteristic of an *entity* (3.1.11) is correct

3.1.5

authenticity

property that an *entity* (3.1.11) is what it claims to be

3.1.6

chain of custody

demonstrable possession, movement, handling and location of material from one point in time until another

Note 1 to entry: Material includes information and other associated *assets* (3.1.2) in the context of ISO/IEC 27002.

[SOURCE: ISO/IEC 27050-1:2019, 3.1, modified — “Note 1 to entry” added]

3.1.7

confidential information

information that is not intended to be made available or disclosed to unauthorized individuals, *entities* (3.1.11) or *processes* (3.1.27)

3.1.8

control

measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any *process* (3.1.27), *policy* (3.1.24), device, practice or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.1.9

disruption

incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives

[SOURCE: ISO 22301:2019, 3.10]

3.1.10

endpoint device

network connected information and communication technology (ICT) hardware device

Note 1 to entry: Endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and Internet of things (IoT) devices.

3.1.11

entity

item relevant for the purpose of operation of a domain that has recognizably distinct existence

Note 1 to entry: An entity can have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12

information processing facility

any information processing system, service or infrastructure, or the physical location housing it

[SOURCE: ISO/IEC 27000:2018, 3.27, modified — "facilities" has been replaced with facility.]

3.1.13

information security breach

compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

3.1.14

information security event

occurrence indicating a possible *information security breach* (3.1.13) or failure of *controls* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — "breach of information security" has been replaced with "information security breach"]

3.1.15

information security incident

one or multiple related and identified *information security events* (3.1.14) that can harm an organization's *assets* (3.1.2) or compromise its operations

[SOURCE: ISO/IEC 27035-1:2016, 3.4]

3.1.16

information security incident management

exercise of a consistent and effective approach to the handling of *information security incidents* (3.1.15)

[SOURCE: ISO/IEC 27035-1:2016, 3.5]

3.1.17

information system

set of applications, services, information technology *assets* (3.1.2), or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.1.18

interested party

stakeholder

person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 27000:2018, 3.37]

3.1.19

non-repudiation

ability to prove the occurrence of a claimed event or action and its originating *entities* (3.1.11)

3.1.20

personnel

persons doing work under the organization's direction

Note 1 to entry: The concept of personnel includes the organization's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.

3.1.21

personally identifiable information

PII

any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The “natural person” in the definition is the *PII principal* (3.1.22). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22

PII principal

natural person to whom the *personally identifiable information (PII)* (3.1.21) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.1.23

PII processor

privacy stakeholder that processes *personally identifiable information (PII)* (3.1.21) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.1.24

policy

intentions and direction of an organization, as formally expressed by its top management

[SOURCE: ISO/IEC 27000:2018, 3.53]

3.1.25

privacy impact assessment

PIA

overall *process* (3.1.27) of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information (PII)* (3.1.21), framed within an organization’s broader risk management framework

[SOURCE: ISO/IEC 29134:2017, 3.7, modified — Note 1 to entry removed.]

3.1.26

procedure

specified way to carry out an activity or a *process* (3.1.27)

[SOURCE: ISO 30000:2009, 3.12]

3.1.27

process

set of interrelated or interacting activities that uses or transforms inputs to deliver a result

[SOURCE: ISO 9000:2015, 3.4.1, modified— Notes to entry removed.]

3.1.28

record

information created, received and maintained as evidence and as an *asset* (3.1.2) by an organization or person, in pursuit of legal obligations or in the transaction of business

Note 1 to entry: Legal obligations in this context include all legal, statutory, regulatory and contractual requirements.

[SOURCE: ISO 15489-1:2016, 3.14, modified— “Note 1 to entry” added.]

3.1.29

recovery point objective

RPO

point in time to which data are to be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.12, modified — “must” replaced by “are to be”.]

3.1.30

recovery time objective

RTO

period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions are to be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.13, modified — “must” replaced by “are to be”.]

3.1.31

reliability

property of consistent intended behaviour and results

3.1.32

rule

accepted principle or instruction that states the organization’s expectations on what is required to be done, what is allowed or not allowed

Note 1 to entry: Rules can be formally expressed in *topic-specific policies* (3.1.35) and in other types of documents.

3.1.33

sensitive information

information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety

3.1.34

threat

potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.1.35

topic-specific policy

intentions and direction on a specific subject or topic, as formally expressed by the appropriate level of management

Note 1 to entry: Topic-specific policies can formally express *rules* (3.1.32) or organization standards.

Note 2 to entry: Some organizations use other terms for these topic-specific policies.

Note 3 to entry: The topic-specific policies referred to in this document are related to information security.

EXAMPLE Topic-specific policy on *access control* (3.1.1), topic-specific policy on clear desk and clear screen.

3.1.36

user

interested party (3.1.18) with access to the organization’s *information systems* (3.1.17)

EXAMPLE *Personnel* (3.1.20), customers, suppliers.

3.1.37

user endpoint device

endpoint device (3.1.10) used by users to access information processing services

Note 1 to entry: User endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, etc.

3.1.38

vulnerability

weakness of an *asset* (3.1.2) or *control* (3.1.8) that can be exploited by one or more *threats* (3.1.34)

[SOURCE: ISO/IEC 27000:2018, 3.77]

3.2 Abbreviated terms

ABAC	attribute-based access control
ACL	access control list
BIA	business impact analysis
BYOD	bring your own device
CAPTCHA	completely automated public Turing test to tell computers and humans apart
CPU	central processing unit
DAC	discretionary access control
DNS	domain name system
GPS	global positioning system
IAM	identity and access management
ICT	information and communication technology
ID	identifier
IDE	integrated development environment
IDS	intrusion detection system
IoT	internet of things
IP	internet protocol
IPS	intrusion prevention system
IT	information technology
ISMS	information security management system
MAC	mandatory access control
NTP	network time protocol
PIA	privacy impact assessment
PII	personally identifiable information

PIN	personal identification number
PKI	public key infrastructure
PTP	precision time protocol
RBAC	role-based access control
RPO	recovery point objective
RTO	recovery time objective
SAST	static application security testing
SD	secure digital
SDN	software-defined networking
SD-WAN	software-defined wide area networking
SIEM	security information and event management
SMS	short message service
SQL	structured query language
SSO	single sign on
SWID	software identification
UEBA	user and entity behaviour analytics
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
VM	virtual machine
VPN	virtual private network
WiFi	wireless fidelity

4 Structure of this document

4.1 Clauses

This document is structured as follows:

- a) Organizational controls (Clause 5)
- b) People controls (Clause 6)
- c) Physical controls (Clause 7)
- d) Technological controls (Clause 8)

There are 2 informative annexes:

- Annex A — Using attributes

— Annex B — Correspondence with ISO/IEC 27002:2013

Annex A explains how an organization can use attributes (see 4.2) to create its own views based on the control attributes defined in this document or of its own creation.

Annex B shows the correspondence between the controls in this edition of ISO/IEC 27002 and the previous 2013 edition.

4.2 Themes and attributes

The categorization of controls given in Clauses 5 to 8 are referred to as themes.

Controls are categorized as:

- a) people, if they concern individual people;
- b) physical, if they concern physical objects;
- c) technological, if they concern technology;
- d) otherwise they are categorized as organizational.

The organization can use attributes to create different views which are different categorizations of controls as seen from a different perspective to the themes. Attributes can be used to filter, sort or present controls in different views for different audiences. Annex A explains how this can be achieved and provides an example of a view.

By way of example, each control in this document has been associated with five attributes with corresponding attribute values (preceded by "#" to make them searchable), as follows:

a) Control type

Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident. Attribute values consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

b) Information security properties

Information security properties is an attribute to view controls from the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of Confidentiality, Integrity and Availability.

c) Cybersecurity concepts

Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of Identify, Protect, Detect, Respond and Recover.

d) Operational capabilities

Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of Governance, Asset_management, Information_protection, Human_resource_security, Physical_security, System_and_network_security, Application_security, Secure_configuration, Identity_and_access_management, Threat_and_vulnerability_management, Continuity, Supplier_relationships_security, Legal_and_compliance, Information_security_event_management and Information_security_assurance.

e) Security domains

Security domains is an attribute to view controls from the perspective of four information security domains: “Governance and Ecosystem” includes “Information System Security Governance & Risk Management” and “Ecosystem cybersecurity management” (including internal and external stakeholders); “Protection” includes “IT Security Architecture”, “IT Security Administration”, “Identity and access management”, “IT Security Maintenance” and “Physical and environmental security”; “Defence” includes “Detection” and “Computer Security Incident Management”; “Resilience” includes “Continuity of operations” and “Crisis management”. Attribute values consist of Governance_and_Ecosystem, Protection, Defence and Resilience.

The attributes given in this document are selected because they are considered generic enough to be used by different types of organizations. Organizations can choose to disregard one or more of the attributes given in this document. They can also create attributes of their own (with the corresponding attribute values) to create their own organizational views. Clause A.2 includes examples of such attributes.

4.3 Control layout

The layout for each control contains the following:

- **Control title:** Short name of the control;
- **Attribute table:** A table shows the value(s) of each attribute for the given control;
- **Control:** What the control is;
- **Purpose:** Why the control should be implemented;
- **Guidance:** How the control should be implemented;
- **Other information:** Explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text. Subheadings are underlined.

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

Guidance

At the highest level, the organization should define an “information security policy” which is approved by top management and which sets out the organization’s approach to managing its information security.

The information security policy should take into consideration requirements derived from:

- a) business strategy and requirements;
- b) regulations, legislation and contracts;
- c) the current and projected information security risks and threats.

The information security policy should contain statements concerning:

- a) definition of information security;
- b) information security objectives or the framework for setting information security objectives;
- c) principles to guide all activities relating to information security;
- d) commitment to satisfy applicable requirements related to information security;
- e) commitment to continual improvement of the information security management system;
- f) assignment of responsibilities for information security management to defined roles;
- g) procedures for handling exemptions and exceptions.

Top management should approve any changes to the information security policy.

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.

Examples of such topics include:

- a) access control;
- b) physical and environmental security;
- c) asset management;
- d) information transfer;
- e) secure configuration and handling of user endpoint devices;
- f) networking security;
- g) information security incident management;
- h) backup;
- i) cryptography and key management;
- j) information classification and handling;
- k) management of technical vulnerabilities;
- l) secure development.

The responsibility for the development, review and approval of the topic-specific policies should be allocated to relevant personnel based on their appropriate level of authority and technical competency. The review should include assessing opportunities for improvement of the organization's information security policy and topic-specific policies and managing information security in response to changes to:

- a) the organization's business strategy;
- b) the organization's technical environment;
- c) regulations, statutes, legislation and contracts;
- d) information security risks;
- e) the current and projected information security threat environment;
- f) lessons learned from information security events and incidents.

The review of information security policy and topic-specific policies should take the results of management reviews and audits into account. Review and update of other related policies should be considered when one policy is changed to maintain consistency.

The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible and understandable to the intended reader. Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable. The organization can determine the formats and names of these policy documents that meet the organization's needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.

If the information security policy or any topic-specific policy is distributed outside the organization, care should be taken not to improperly disclose confidential information.

Table 1 illustrates the differences between information security policy and topic-specific policy.

Table 1 — Differences between information security policy and topic-specific policy

	Information security policy	Topic-specific policy
Level of detail	General or high-level	Specific and detailed
Documented and formally approved by	Top management	Appropriate level of management

Other information

Topic-specific policies can vary across organizations.

5.2 Information security roles and responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosys-tem #Protection #Resilience

Control

Information security roles and responsibilities should be defined and allocated according to the organization needs.

Purpose

To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

Guidance

Allocation of information security roles and responsibilities should be done in accordance with the information security policy and topic-specific policies (see 5.1). The organization should define and manage responsibilities for:

- a) protection of information and other associated assets;
- b) carrying out specific information security processes;
- c) information security risk management activities and in particular acceptance of residual risks (e.g. to risk owners);
- d) all personnel using an organization's information and other associated assets.

These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Individuals with allocated information security responsibilities can assign security tasks to others. However, they remain accountable and should determine that any delegated tasks have been correctly performed.

Each security area for which individuals are responsible should be defined, documented and communicated. Authorization levels should be defined and documented. Individuals who take on a specific information security role should be competent in the knowledge and skills required by the role and should be supported to keep up to date with developments related to the role and required in order to fulfil the responsibilities of the role.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of risks and mitigating controls.

However, responsibility for resourcing and implementing the controls often remains with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

Depending on the size and resourcing of an organization, information security can be covered by dedicated roles or duties carried out in addition to existing roles.

5.3 Segregation of duties

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem

Control

Conflicting duties and conflicting areas of responsibility should be segregated.

Purpose

To reduce the risk of fraud, error and bypassing of information security controls.

Guidance

Segregation of duties and areas of responsibility aims to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own.

The organization should determine which duties and areas of responsibility need to be segregated. The following are examples of activities that can require segregation:

- a) initiating, approving and executing a change;
- b) requesting, approving and implementing access rights;
- c) designing, implementing and reviewing code;
- d) developing software and administering production systems;
- e) using and administering applications;
- f) using applications and administering databases;
- g) designing, auditing and assuring information security controls.

The possibility of collusion should be considered in designing the segregation controls. Small organizations can find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls should be considered, such as monitoring of activities, audit trails and management supervision.

Care should be taken when using role-based access control systems to ensure that persons are not granted conflicting roles. When there is a large number of roles, the organization should consider using automated tools to identify conflicts and facilitate their removal. Roles should be carefully defined and provisioned to minimize access problems if a role is removed or reassigned.

Other information

No other information.

5.4 Management responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

Control

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

Guidance

Management should demonstrate support of the information security policy, topic-specific policies, procedures and information security controls.

Management responsibilities should include ensuring that personnel:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets;

- b) are provided with guidelines which state the information security expectations of their role within the organization;
- c) are mandated to fulfil the information security policy and topic-specific policies of the organization;
- d) achieve a level of awareness of information security relevant to their roles and responsibilities within the organization (see 6.3);
- e) compliance with the terms and conditions of employment, contract or agreement, including the organization's information security policy and appropriate methods of working;
- f) continue to have the appropriate information security skills and qualifications through ongoing professional education;
- g) where practicable, are provided with a confidential channel for reporting violations of information security policy, topic-specific policies or procedures for information security (“whistleblowing”). This can allow for anonymous reporting, or have provisions to ensure that knowledge of the identity of the reporter is known only to those who need to deal with such reports;
- h) are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.

Other information

No other information.

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control

The organization should establish and maintain contact with relevant authorities.

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information

Organizations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be a requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity processes (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in

connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment)].

5.6 Contact with special interest groups

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

Control

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Purpose

To ensure appropriate flow of information takes place with respect to information security.

Guidance

Membership of special interest groups or forums should be considered as a means to:

- improve knowledge about best practices and stay up to date with relevant security information;
- ensure the understanding of the information security environment is current;
- receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
- gain access to specialist information security advice;
- share and exchange information about new technologies, products, services, threats or vulnerabilities;
- provide suitable liaison points when dealing with information security incidents (see 5.24 to 5.28).

Other information

No other information.

5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

Guidance

Information about existing or emerging threats is collected and analysed in order to:

- a) facilitate informed actions to prevent the threats from causing harm to the organization;
- b) reduce the impact of such threats.

Threat intelligence can be divided into three layers, which should all be considered:

- a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks);
- b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved;
- c) operational threat intelligence: details about specific attacks, including technical indicators.

Threat intelligence should be:

- a) relevant (i.e. related to the protection of the organization);
- b) insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);
- c) contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);
- d) actionable (i.e. the organization can act on information quickly and effectively).

Threat intelligence activities should include:

- a) establishing objectives for threat intelligence production;
- b) identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence;
- c) collecting information from selected sources, which can be internal and external;
- d) processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information);
- e) analysing information to understand how it relates and is meaningful to the organization;
- f) communicating and sharing it to relevant individuals in a format that can be understood.

Threat intelligence should be analysed and later used:

- a) by implementing processes to include information gathered from threat intelligence sources into the organization's information security risk management processes;
- b) as additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions;
- c) as input to the information security test processes and techniques.

The organization should share threat intelligence with other organizations on a mutual basis in order to improve overall threat intelligence.

Other information

Organizations can use threat intelligence to prevent, detect, or respond to threats. Organizations can produce threat intelligence, but more typically receive and make use of threat intelligence produced by other sources.

Threat intelligence is often provided by independent providers or advisors, government agencies or collaborative threat intelligence groups.

The effectiveness of controls such as 5.25, 8.7, 8.16 or 8.23, depends on the quality of available threat intelligence.

5.8 Information security in project management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection

Control

Information security should be integrated into project management.

Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.

Guidance

Information security should be integrated into project management to ensure information security risks are addressed as part of the project management. This can be applied to any type of project regardless of its complexity, size, duration, discipline or application area (e.g. a project for a core business process, ICT, facility management or other supporting processes).

The project management in use should require that:

- information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle;
- information security requirements [e.g. application security requirements (8.26), requirements for complying with intellectual property rights (5.32), etc.] are addressed in the early stages of projects;
- information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle;
- progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested.

The appropriateness of the information security considerations and activities should be followed up at predefined stages by suitable persons or governance bodies, such as the project steering committee.

Responsibilities and authorities for information security relevant to the project should be defined and allocated to specified roles.

Information security requirements for products or services to be delivered by the project should be determined using various methods, including deriving compliance requirements from information security policy, topic-specific policies and regulations. Further information security requirements can be derived from activities such as threat modelling, incident reviews, use of vulnerability thresholds or contingency planning, thus ensuring that the architecture and design of information systems are protected against known threats based on the operational environment.

Information security requirements should be determined for all types of projects, not only ICT development projects. The following should also be considered when determining these requirements:

- a) what information is involved (information determination), what are the corresponding information security needs (classification; see 5.12) and the potential negative business impact which can result from lack of adequate security;
- b) the required protection needs of information and other associated assets involved, particularly in terms of confidentiality, integrity and availability;
- c) the level of confidence or assurance required towards the claimed identity of entities in order to derive the authentication requirements;
- d) access provisioning and authorization processes, for customers and other potential business users as well as for privileged or technical users such as relevant project members, potential operation staff or external suppliers;
- e) informing users of their duties and responsibilities;
- f) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;
- g) requirements mandated by other information security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
- h) compliance with the legal, statutory, regulatory and contractual environment in which the organization operates;
- i) level of confidence or assurance required for third parties to meet the organization's information security policy and topic-specific policies including relevant security clauses in any agreements or contracts.

Other information

The project development approach, such as waterfall life cycle or agile life cycle, should support information security in a structured way that can be adapted to suit the assessed severity of the information security risks, based on the character of the project. Early consideration of information security requirements for the product or service (e.g. at the planning and design stages), can lead to more effective and cost-efficient solutions for quality and information security. ISO 21500 and ISO 21502 provide guidance on concepts and processes of project management that are important for the performance of projects.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Control

An inventory of information and other associated assets, including owners, should be developed and maintained.

Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

Guidance

Inventory

The organization should identify its information and other associated assets and determine their importance in terms of information security. Documentation should be maintained in dedicated or existing inventories as appropriate.

The inventory of information and other associated assets should be accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information and other associated assets include:

- a) conducting regular reviews of identified information and other associated assets against the asset inventory;
- b) automatically enforcing an inventory update in the process of installing, changing or removing an asset.

The location of an asset should be included in the inventory as appropriate.

The inventory does not need to be a single list of information and other associated assets. Considering that the inventory should be maintained by the relevant functions, it can be seen as a set of dynamic inventories, such as inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competence, capabilities and records.

Each asset should be classified in accordance with the classification of the information (see 5.12) associated to that asset.

The granularity of the inventory of information and other associated assets should be at a level appropriate for the needs of the organization. Sometimes specific instances of assets in the information life cycle are not feasible to be documented due to the nature of the asset. An example of a short-lived asset is a VM instance whose life cycle can be of short duration.

Ownership

For the identified information and other associated assets, ownership of the asset should be assigned to an individual or a group and the classification should be identified (see 5.12, 5.13). A process to ensure timely assignment of asset ownership should be implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. Asset ownership should be reassigned as necessary when current asset owners leave or change job roles.

Owner duties

The asset owner should be responsible for the proper management of an asset over the whole asset life cycle, ensuring that:

- a) information and other associated assets are inventoried;
- b) information and other associated assets are appropriately classified and protected;
- c) the classification is reviewed periodically;
- d) components supporting technology assets are listed and linked, such as database, storage, software components and sub-components;
- e) requirements for the acceptable use of information and other associated assets (see 5.10) are established;
- f) access restrictions correspond with the classification and that they are effective and are reviewed periodically;
- g) information and other associated assets, when deleted or disposed, are handled in a secure manner and removed from the inventory;

- h) they are involved in the identification and management of risks associated with their asset(s);
- i) they support personnel who have the roles and responsibilities of managing their information.

Other information

Inventories of information and other associated assets are often necessary to ensure the effective protection of information and can be required for other purposes, such as health and safety, insurance or financial reasons. Inventories of information and other associated assets also support risk management, audit activities, vulnerability management, incident response and recovery planning.

Tasks and responsibilities can be delegated (e.g. to a custodian looking after the assets on a daily basis), but the person or group who delegated them remains accountable.

It can be useful to designate groups of information and other associated assets which act together to provide a particular service. In this case, the owner of this service is accountable for the delivery of the service, including the operation of its assets.

See ISO/IEC 19770-1 for additional information on information technology (IT) asset management. See ISO 55001 for additional information on asset management.

5.10 Acceptable use of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection

Control

Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

Purpose

To ensure information and other associated assets are appropriately protected, used and handled.

Guidance

Personnel and external party users using or having access to the organization's information and other associated assets should be made aware of the information security requirements for protecting and handling the organization's information and other associated assets. They should be responsible for their use of any information processing facilities.

The organization should establish a topic-specific policy on the acceptable use of information and other associated assets and communicate it to anyone who uses or handles information and other associated assets. The topic-specific policy on acceptable use should provide clear direction on how individuals are expected to use information and other associated assets. The topic-specific policy should state:

- a) expected and unacceptable behaviours of individuals from an information security perspective;
- b) permitted and prohibited use of information and other associated assets;
- c) monitoring activities being performed by the organization.

Acceptable use procedures should be drawn up for the full information life cycle in accordance with its classification (see 5.12) and determined risks. The following items should be considered:

- a) access restrictions supporting the protection requirements for each level of classification;
- b) maintenance of a record of the authorized users of information and other associated assets;

- c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
- d) storage of assets associated with information in accordance with manufacturers' specifications (see 7.8);
- e) clear marking of all copies of storage media (electronic or physical) for the attention of the authorized recipient (see 7.10);
- f) authorization of disposal of information and other associated assets and supported deletion method(s) (see 8.10).

Other information

It can be the case that the assets concerned do not directly belong to the organization, such as public cloud services. The use of such third-party assets and any assets of the organization associated with such external assets (e.g. information, software) should be identified as applicable and controlled, for example, through agreements with cloud service providers. Care should also be taken when a collaborative working environment is used.

5.11 Return of assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

Control

Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Purpose

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

Guidance

The change or termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where personnel and other interested parties purchase the organization's equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment (see 7.14).

In cases where personnel and other interested parties have knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period and thereafter, the organization should prevent unauthorized copying of relevant information (e.g. intellectual property) by personnel under notice of termination.

The organization should clearly identify and document all information and other associated assets to be returned which can include:

- a) user endpoint devices;
- b) portable storage devices;
- c) specialist equipment;

- d) authentication hardware (e.g. mechanical keys, physical tokens and smartcards) for information systems, sites and physical archives;
- e) physical copies of information.

Other information

It can be difficult to return information held on assets which are not owned by the organization. In such cases, it is necessary to restrict the use of information using other information security controls such as access rights management (5.18) or use of cryptography (8.24).

5.12 Classification of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

Guidance

The organization should establish a topic-specific policy on information classification and communicate it to all relevant interested parties.

The organization should take into account requirements for confidentiality, integrity and availability in the classification scheme.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, for protecting integrity of information and for assuring availability, as well as legal requirements concerning the confidentiality, integrity or availability of the information. Assets other than information can also be classified in compliance with classification of information, which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. Results of classification should be updated in accordance with changes of the value, sensitivity and criticality of information through their life cycle.

The scheme should be aligned to the topic-specific policy on access control (see 5.1) and should be able to address specific business needs of the organization.

The classification can be determined by the level of impact that the information's compromise would have for the organization. Each level defined in the scheme should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization and included in its procedures so that everyone classifies information and applicable other associated assets in the same way. In this manner, everyone has a common understanding of protection requirements and applies appropriate protection.

The classification scheme used within the organization can be different from the schemes used by other organizations, even if the names for levels are similar. In addition, information moving between

organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical. Therefore, agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification levels from other organizations. Correspondence between different schemes can be determined by looking for equivalence in the associated handling and protection methods.

Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time. For example, when the information has been made public, it no longer has confidentiality requirements but can still require protection for its integrity and availability properties. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or, on the contrary, under-classification can lead to insufficient controls to protect the information from compromise.

As an example, an information confidentiality classification scheme can be based on four levels as follows:

- a) disclosure causes no harm;
- b) disclosure causes minor reputational damage or minor operational impact;
- c) disclosure has a significant short-term impact on operations or business objectives;
- d) disclosure has a serious impact on long term business objectives or puts the survival of the organization at risk.

5.13 Labelling of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Purpose

To facilitate the communication of classification of information and support automation of information processing and management.

Guidance

Procedures for information labelling should cover information and other associated assets in all formats. The labelling should reflect the classification scheme established in 5.12. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of storage media. The procedures can define:

- a) cases where labelling is omitted (e.g. labelling of non-confidential information to reduce workloads);
- b) how to label information sent by or stored on electronic or physical means, or any other format;

c) how to handle cases where labelling is not possible (e.g. due to technical restrictions).

Examples of labelling techniques include:

- a) physical labels;
- b) headers and footers;
- c) metadata;
- d) watermarking;
- e) rubber-stamps.

Digital information should utilize metadata in order to identify, manage and control information, especially with regard to confidentiality. Metadata should also enable efficient and correct searching for information. Metadata should facilitate systems to interact and make decisions based on the associated classification labels.

The procedures should describe how to attach metadata to information, what labels to use and how data should be handled, in line with the organization's information model and ICT architecture.

Relevant additional metadata should be added by systems when they process information depending on its information security properties.

Personnel and other interested parties should be made aware of labelling procedures. All personnel should be provided with the necessary training to ensure that information is correctly labelled and handled accordingly.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing.

Other useful metadata that can be attached to the information is which organizational process created the information and at what time.

Labelling of information and other associated assets can sometimes have negative effects. Classified assets can be easier to identify by malicious actors for potential misuse.

Some systems do not label individual files or database records with their classification but protect all information at the highest level of classification of any of the information that it contains or is permitted to contain. It is usual in such systems to determine and then label information when it is exported.

5.14 Information transfer

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

Purpose

To maintain the security of information transferred within an organization and with any external interested party.

Guidance

General

The organization should establish and communicate a topic-specific policy on information transfer to all relevant interested parties. Rules, procedures and agreements to protect information in transit should reflect the classification of the information involved. Where information is transferred between the organization and third parties, transfer agreements (including recipient authentication) should be established and maintained to protect information in all forms in transit (see 5.10).

Information transfer can happen through electronic transfer, physical storage media transfer and verbal transfer.

For all types of information transfer, rules, procedures and agreements should include:

- a) controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the classification of the information involved and any special controls that are required to protect sensitive information, such as use of cryptographic techniques (see 8.24);
- b) controls to ensure traceability and non-repudiation, including maintaining a chain of custody for information while in transit;
- c) identification of appropriate contacts related to the transfer including information owners, risk owners, security officers and information custodians, as applicable;
- d) responsibilities and liabilities in the event of information security incidents, such as loss of physical storage media or data;
- e) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 5.13);
- f) reliability and availability of the transfer service;
- g) the topic-specific policy or guidelines on acceptable use of information transfer facilities (see 5.10);
- h) retention and disposal guidelines for all business records, including messages;

NOTE Local legislation and regulations can exist regarding retention and disposal of business records.

- i) the consideration of any other relevant legal, statutory, regulatory and contractual requirements (see 5.31, 5.32, 5.33, 5.34) related to transfer of information (e.g. requirements for electronic signatures).

Electronic transfer

Rules, procedures and agreements should also consider the following items when using electronic communication facilities for information transfer:

- a) detection of and protection against malware that can be transmitted through the use of electronic communications (see 8.7);
- b) protection of communicated sensitive electronic information that is in the form of an attachment;
- c) prevention against sending documents and messages in communications to the wrong address or number;

- d) obtaining approval prior to using external public services such as instant messaging, social networking, file sharing or cloud storage;
- e) stronger levels of authentication when transferring information via publicly accessible networks;
- f) restrictions associated with electronic communication facilities (e.g. preventing automatic forwarding of electronic mail to external mail addresses);
- g) advising personnel and other interested parties not to send short message service (SMS) or instant messages with critical information since these can be read in public places (and therefore by unauthorized persons) or stored in devices not adequately protected;
- h) advising personnel and other interested parties about the problems of using fax machines or services, namely:
 - 1) unauthorized access to built-in message stores to retrieve messages;
 - 2) deliberate or accidental programming of machines to send messages to specific numbers.

Physical storage media transfer

When transferring physical storage media (including paper), rules, procedures and agreements should also include:

- a) responsibilities for controlling and notifying transmission, dispatch and receipt;
- b) ensuring correct addressing and transportation of the message;
- c) packaging that protects the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that can reduce the effectiveness of restoring storage media such as exposure to heat, moisture or electromagnetic fields; using minimum technical standards for packaging and transmission (e.g. the use of opaque envelopes);
- d) a list of authorized reliable couriers agreed by management;
- e) courier identification standards;
- f) depending on the classification level of the information in the storage media to be transported, use tamper evident or tamper-resistant controls (e.g. bags, containers);
- g) procedures to verify the identification of couriers;
- h) approved list of third parties providing transportation or courier services depending on the classification of the information;
- i) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination.

Verbal transfer

To protect verbal transfer of information, personnel and other interested parties should be reminded that they should:

- a) not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorized persons;
- b) not leave messages containing confidential information on answering machines or voice messages since these can be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;
- c) be screened to the appropriate level to listen to the conversation;

- d) ensure that appropriate room controls are implemented (e.g. sound-proofing, closed door);
- e) begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.

Other information

No other information.

5.15 Access control

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Purpose

To ensure authorized access and to prevent unauthorized access to information and other associated assets.

Guidance

Owners of information and other associated assets should determine information security and business requirements related to access control. A topic-specific policy on access control should be defined which takes account of these requirements and should be communicated to all relevant interested parties.

These requirements and the topic-specific policy should consider the following:

- a) determining which entities require which type of access to the information and other associated assets;
- b) security of applications (see 8.26);
- c) physical access, which needs to be supported by appropriate physical entry controls (see 7.2, 7.3, 7.4);
- d) information dissemination and authorization (e.g. the need-to-know principle) and information security levels and classification of information (see 5.10, 5.12, 5.13);
- e) restrictions to privileged access (see 8.2);
- f) segregation of duties (see 5.3);
- g) relevant legislation, regulations and any contractual obligations regarding limitation of access to data or services (see 5.31, 5.32, 5.33, 5.34, 8.3);
- h) segregation of access control functions (e.g. access request, access authorization, access administration);
- i) formal authorization of access requests (see 5.16 and 5.18);
- j) the management of access rights (see 5.18);
- k) logging (see 8.15).

Access control rules should be implemented by defining and mapping appropriate access rights and restrictions to the relevant entities (see 5.16). An entity can represent a human user as well as a technical or logical item (e.g. a machine, device or a service). To simplify the access control management, specific roles can be assigned to entity groups.

The following should be taken into account when defining and implementing access control rules:

- a) consistency between the access rights and information classification;
- b) consistency between the access rights and the physical perimeter security needs and requirements;
- c) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use;
- d) considering how elements or factors relevant to dynamic access control can be reflected.

Other information

There are often overarching principles used in the context of access control. Two of the most frequently used principles are:

- a) need-to-know: an entity is only granted access to the information which that entity requires in order to perform its tasks (different tasks or roles mean different need-to-know information and hence different access profiles);
- b) need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.

Care should be taken when specifying access control rules to consider:

- a) establishing rules based on the premise of least privilege, “Everything is generally forbidden unless expressly permitted”, rather than the weaker rule, “Everything is generally permitted unless expressly forbidden”;
- b) changes in information labels (see 5.13) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
- c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
- d) when to define and regularly review the approval.

Access control rules should be supported by documented procedures (see 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) and defined responsibilities (see 5.2, 5.17).

There are several ways to implement access control, such as MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control) and ABAC (attribute-based access control).

Access control rules can also contain dynamic elements (e.g. a function that evaluates past accesses or specific environment values). Access control rules can be implemented in different granularity, ranging from covering whole networks or systems to specific data fields and can also consider properties such as user location or the type of network connection that is used for access. These principles and how granular access control is defined can have a significant cost impact. Stronger rules and more granularity typically lead to higher cost. Business requirements and risk considerations should be used to define which access control rules are applied and which granularity is required.

5.16 Identity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

The full life cycle of identities should be managed.

Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

Guidance

The processes used in the context of identity management should ensure that:

- for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity;
- identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval and documentation;
- identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight;
- identities are disabled or removed in a timely fashion if they are no longer required (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the organization or changed the role);
- in a specific domain, a single identity is mapped to a single entity, [i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided];
- records of all significant events concerning the use and management of user identities and of authentication information are kept.

The organization should have a supporting process in place to handle changes to information related to user identities. These processes can include re-verification of trusted documents related to a person.

When using identities provided or issued by third parties (e.g. social media credentials), the organization should ensure the third-party identities provide the required trust level and any associated risks are known and sufficiently treated. This can include controls related to the third parties (see 5.19) as well as controls related to associated authentication information (see 5.17).

Other information

Providing or revoking access to information and other associated assets is usually a multi-step procedure:

- confirming the business requirements for an identity to be established;
- verifying the identity of an entity before allocating them a logical identity;
- establishing an identity;
- configuring and activating the identity. This also includes configuration and initial setup of related authentication services;

- e) providing or revoking specific access rights to the identity, based on appropriate authorization or entitlement decisions (see 5.18).

5.17 Authentication information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

Purpose

To ensure proper entity authentication and prevent failures of authentication processes.

Guidance

Allocation of authentication information

The allocation and management process should ensure that:

- personal passwords or personal identification numbers (PINs) generated automatically during enrolment processes as temporary secret authentication information are non-guessable and unique for each person, and that users are required to change them after the first use;
- procedures are established to verify the identity of a user prior to providing new, replacement or temporary authentication information;
- authentication information, including temporary authentication information, is transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected (clear text) electronic mail messages for this purpose is avoided;
- users acknowledge receipt of authentication information;
- default authentication information as predefined or provided by vendors is changed immediately following installation of systems or software;
- records of significant events concerning allocation and management of authentication information are kept and their confidentiality is granted, and that the record-keeping method is approved (e.g. by using an approved password vault tool).

User responsibilities

Any person having access to or using authentication information should be advised to ensure that:

- secret authentication information such as passwords are kept confidential. Personal secret authentication information is not to be shared with anyone. Secret authentication information used in the context of identities linked to multiple users or linked to non-personal entities are solely shared with authorized persons;
- affected or compromised authentication information is changed immediately upon notification of or any other indication of a compromise;

- c) when passwords are used as authentication information, strong passwords according to best practice recommendations are selected, for example:
 - 1) passwords are not based on anything somebody else can easily guess or obtain using person-related information (e.g. names, telephone numbers and dates of birth);
 - 2) passwords are not based on dictionary words or combinations thereof;
 - 3) use easy to remember passphrases and try to include alphanumerical and special characters;
 - 4) passwords have a minimum length;
- d) the same passwords are not used across distinct services and systems;
- e) the obligation to follow these rules is also included in terms and conditions of employment (see 6.2).

Password management system

When passwords are used as authentication information, the password management system should:

- a) allow users to select and change their own passwords and include a confirmation procedure to address input errors;
- b) enforce strong passwords according to good practice recommendations [see c) of "User responsibilities];
- c) force users to change their passwords at first login;
- d) enforce password changes as necessary, for example after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);
- e) prevent re-use of previous passwords;
- f) prevent the use of commonly-used passwords and compromised usernames, password combinations from hacked systems;
- g) not display passwords on the screen when being entered;
- h) store and transmit passwords in protected form.

Password encryption and hashing should be performed according to approved cryptographic techniques for passwords (see 8.24).

Other information

Passwords or passphrases are a commonly used type of authentication information and are a common means of verifying a user's identity. Other types of authentication information are cryptographic keys, data stored on hardware tokens (e.g. smart cards) that produce authentication codes and biometric data such as iris scans or fingerprints. Additional information can be found in the ISO/IEC 24760 series.

Requiring frequent change of passwords can be problematic because users can get annoyed by the frequent changes, forget new passwords, note them down in unsafe places, or choose unsafe passwords. Provision of single sign on (SSO) or other authentication management tools (e.g. password vaults) reduces the amount of authentication information that users are required to protect and can thereby increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of authentication information.

Some applications require user passwords to be assigned by an independent authority. In such cases, a), c) and d) of "Password management system" do not apply.

5.18 Access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

Guidance

Provision and revocation of access rights

The provisioning process for assigning or revoking physical and logical access rights granted to an entity's authenticated identity should include:

- obtaining authorization from the owner of the information and other associated assets for the use of the information and other associated assets (see 5.9). Separate approval for access rights by management can also be appropriate;
- considering the business requirements and the organization's topic-specific policy and rules on access control;
- considering segregation of duties, including segregating the roles of approval and implementation of the access rights and separation of conflicting roles;
- ensuring access rights are removed when someone does not need to access the information and other associated assets, in particular ensuring access rights of users who have left the organization are removed in a timely fashion;
- considering giving temporary access rights for a limited time period and revoking them at the expiration date, in particular for temporary personnel or temporary access required by personnel;
- verifying that the level of access granted is in accordance with the topic-specific policies on access control (see 5.15) and is consistent with other information security requirements such as segregation of duties (see 5.3);
- ensuring that access rights are activated (e.g. by service providers) only after authorization procedures are successfully completed;
- maintaining a central record of access rights granted to a user identifier (ID, logical or physical) to access information and other associated assets;
- modifying access rights of users who have changed roles or jobs;
- removing or adjusting physical and logical access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions;
- maintaining a record of changes to users' logical and physical access rights.

Review of access rights

Regular reviews of physical and logical access rights should consider the following:

- a) users' access rights after any change within the same organization (e.g. job change, promotion, demotion) or termination of employment (see 6.1 to 6.5);
- b) authorizations for privileged access rights.

Consideration before change or termination of employment

A user's access rights to information and other associated assets should be reviewed and adjusted or removed before any change or termination of employment based on the evaluation of risk factors such as:

- a) whether the termination or change is initiated by the user or by management and the reason for termination;
- b) the current responsibilities of the user;
- c) the value of the assets currently accessible.

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews of access rights are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel (see 5.20, 6.2, 6.4, 6.6).

In cases of management-initiated termination, disgruntled personnel or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they can be tempted to collect information for future use.

Cloning is an efficient way for organizations to assign access to users. However, it should be done with care based on distinct roles identified by the organization rather than just cloning an identity with all associated access rights. Cloning has an inherent risk of resulting in excessive access rights to information and other associated assets.

5.19 Information security in supplier relationships

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

Purpose

To maintain an agreed level of information security in supplier relationships.

Guidance

The organization should establish and communicate a topic-specific policy on supplier relationships to all relevant interested parties.

The organization should identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers. This should also apply to the organization's use of resources of cloud service providers. These processes and procedures should include those to be implemented by the organization, as well as those the organization requires the

supplier to implement for the commencement of use of a supplier's products or services or for the termination of use of a supplier's products and services, such as:

- a) identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;
- b) establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, on-site assessments, certifications);
- c) evaluating and selecting supplier's products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier's information and information processing and hence the organization's information security;
- d) defining the organization's information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;
- e) defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information;
- f) assessing and managing the information security risks associated with:
 - 1) the suppliers' use of the organization's information and other associated assets, including risks originating from potential malicious supplier personnel;
 - 2) malfunctioning or vulnerabilities of the products (including software components and sub-components used in these products) or services provided by the suppliers;
- g) monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;
- h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by other means;
- i) handling incidents and contingencies associated with supplier products and services including responsibilities of both the organization and suppliers;
- j) resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier's information and information processing and hence the availability of the organization's information;
- k) awareness and training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement, topic-specific policies, processes and procedures and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
- l) managing the necessary transfer of information, other associated assets and anything else that needs to be changed and ensuring that information security is maintained throughout the transfer period;
- m) requirements to ensure a secure termination of the supplier relationship, including:
 - 1) de-provisioning of access rights;
 - 2) information handling;
 - 3) determining ownership of intellectual property developed during the engagement;
 - 4) information portability in case of change of supplier or insourcing;
 - 6) records management;

- 7) return of assets;
- 8) secure disposal of information and other associated assets;
- 9) ongoing confidentiality requirements;
- n) level of personnel security and physical security expected from supplier's personnel and facilities.

The procedures for continuing information processing in the event that the supplier becomes unable to supply its products or services (e.g. because of an incident, because the supplier is no longer in business, or no longer provides some components due to technology advancements) should be considered to avoid any delay in arranging replacement products or services (e.g. identifying an alternative supplier in advance or always using alternative suppliers).

Other information

In cases where it is not possible for an organization to place requirements on a supplier, the organization should:

- a) consider the guidance given in this control in making decisions about choosing a supplier and its product or service;
- b) implement compensating controls as necessary based on a risk assessment.

Information can be put at risk by suppliers with inadequate information security management. Controls should be determined and applied to manage the supplier's access to information and other associated assets. For example, if there is a special need for confidentiality of the information, non-disclosure agreements or cryptographic techniques can be used. Another example is personal data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

Risks can also be caused by inadequate controls of ICT infrastructure components or services provided by suppliers. Malfunctioning or vulnerable components or services can cause information security breaches in the organization or to another entity (e.g. they can cause malware infection, attacks or other harm on entities other than the organization).

See ISO/IEC 27036-2 for more detail.

5.20 Addressing information security within supplier agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

Purpose

To maintain an agreed level of information security in supplier relationships.

Guidance

Supplier agreements should be established and documented to ensure that there is clear understanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms can be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

- a) description of the information to be provided or accessed and methods of providing or accessing the information;
- b) classification of information according to the organization's classification scheme (see 5.10, 5.12, 5.13);
- c) mapping between the organization's own classification scheme and the classification scheme of the supplier;
- d) legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;
- e) obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting and auditing, and the supplier's obligations to comply with the organization's information security requirements;
- f) rules of acceptable use of information and other associated assets, including unacceptable use if necessary;
- g) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel (e.g. through an explicit list of supplier personnel authorized to use the organization's information and other associated assets);
- h) information security requirements regarding the supplier's ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and risk criteria;
- i) indemnities and remediation for failure of contractor to meet requirements;
- j) incident management requirements and procedures (especially notification and collaboration during incident remediation);
- k) training and awareness requirements for specific procedures and information security requirements (e.g. for incident response, authorization procedures);
- l) relevant provisions for sub-contracting, including the controls that need to be implemented, such as agreement on the use of sub-suppliers (e.g. requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change);
- m) relevant contacts, including a contact person for information security issues;
- n) any screening requirements, where legally permissible, for the supplier's personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;
- o) the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls;
- p) right to audit the supplier processes and controls related to the agreement;
- q) supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
- r) defect resolution and conflict resolution processes;

- s) providing backup aligned with the organization's needs (in terms of frequency and type and storage location);
- t) ensuring the availability of an alternate facility (i.e. disaster recovery site) not subject to the same threats as the primary facility and considerations for fall back controls (alternate controls) in the event primary controls fail;
- u) having a change management process that ensures advance notification to the organization and the possibility for the organization of not accepting changes;
- v) physical security controls commensurate with the information classification;
- w) information transfer controls to protect the information during physical transfer or logical transmission;
- x) termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;
- y) provision of a method of securely destroying the organization's information stored by the supplier as soon as it is no longer required;
- z) ensuring, at the end of the contract, handover support to another supplier or to the organization itself.

The organization should establish and maintain a register of agreements with external parties (e.g. contracts, memorandum of understanding, information-sharing agreements) to keep track of where their information is going. The organization should also regularly review, validate and update their agreements with external parties to ensure they are still required and fit for purpose with relevant information security clauses.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant requirements for addressing information security risks.

For details on supplier agreements, see ISO/IEC 27036 series. For cloud service agreements, see ISO/IEC 19086 series.

5.21 Managing information security in the ICT supply chain

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

Purpose

To maintain an agreed level of information security in supplier relationships.

Guidance

The following topics should be considered to address information security within ICT supply chain security in addition to the general information security requirements for supplier relationships:

- a) defining information security requirements to apply to ICT product or service acquisition;
- b) requiring that ICT services suppliers propagate the organization's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the organization;
- c) requiring that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities (e.g. sub-contracted software developers and hardware component providers);
- d) requesting that ICT products suppliers provide information describing the software components used in products;
- e) requesting that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation;
- f) implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements. Examples of such supplier review methods can include penetration testing and proof or validation of third-party attestations for the supplier's information security operations;
- g) implementing a process for identifying and documenting product or service components that are critical for maintaining functionality and therefore require increased attention, scrutiny and further follow up required when built outside of the organization especially if the supplier outsources aspects of product or service components to other suppliers;
- h) obtaining assurance that critical components and their origin can be traced throughout the supply chain;
- i) obtaining assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features;
- j) implementing processes to ensure that components from suppliers are genuine and unaltered from their specification. Example measures include anti-tamper labels, cryptographic hash verifications or digital signatures. Monitoring for out of specification performance can be an indicator of tampering or counterfeits. Prevention and detection of tampering should be implemented during multiple stages in the system development life cycle, including design, development, integration, operations and maintenance;
- k) obtaining assurance that ICT products achieve required security levels, for example, through formal certification or an evaluation scheme such as the Common Criteria Recognition Arrangement;
- l) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;
- m) implementing specific processes for managing ICT component life cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements. Identification of an alternative supplier and the process to transfer software and competence to the alternative supplier should be considered.

Other information

The specific ICT supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the ICT supply chain and any matters that have an important effect on the products and services being provided. The organization can influence ICT supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the ICT supply chain.

ICT should be acquired from reputable sources. The reliability of software and hardware is a matter of quality control. While it is generally not possible for an organization to inspect the quality control systems of its vendors, it can make reliable judgments based on the reputation of the vendor.

ICT supply chain as addressed here includes cloud services.

Examples of ICT supply chains are:

- a) cloud services provisioning, where the cloud service provider relies on the software developers, telecommunication service providers, hardware providers;
- b) IoT, where the service involves the device manufacturers, the cloud service providers (e.g. the IoT platform operators), the developers for mobile and web applications, the vendor of software libraries;
- c) hosting services, where the provider relies on external service desks including first, second and third support levels.

See ISO/IEC 27036-3 for more details including risk assessment guidance.

Software identification (SWID) tags can also help to achieve better information security in the supply chain, by providing information about software provenance. See ISO/IEC 19770-2 for more details.

5.22 Monitoring, review and change management of supplier services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence

Control

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements.

Guidance

Monitoring, review and change management of supplier services should ensure the information security terms and conditions of the agreements are complied with, information security incidents and problems are managed properly and changes in supplier services or business status do not affect service delivery.

This should involve a process to manage the relationship between the organization and the supplier to:

- a) monitor service performance levels to verify compliance with the agreements;
- b) monitor changes made by suppliers including:
 - 1) enhancements to the current services offered;

- 2) development of any new applications and systems;
- 3) modifications or updates of the supplier's policies and procedures;
- 4) new or changed controls to resolve information security incidents and to improve information security;
- c) monitor changes in supplier services including:
 - 1) changes and enhancement to networks;
 - 2) use of new technologies;
 - 3) adoption of new products or newer versions or releases;
 - 4) new development tools and environments;
 - 5) changes to physical location of service facilities;
 - 6) change of sub-suppliers;
 - 7) sub-contracting to another supplier;
- d) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
- e) conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;
- f) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;
- g) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
- h) respond to and manage any identified information security events or incidents;
- i) identify information security vulnerabilities and manage them;
- j) review information security aspects of the supplier's relationships with its own suppliers;
- k) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 5.29, 5.30, 5.35, 5.36, 8.14);
- l) ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements;
- m) evaluate regularly that the suppliers maintain adequate information security levels.

The responsibility for managing supplier relationships should be assigned to a designated individual or team. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate actions should be taken when deficiencies in the service delivery are observed.

Other information

See ISO/IEC 27036-3 for more detail.

5.23 Information security for use of cloud services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Purpose

To specify and manage information security for the use of cloud services.

Guidance

The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties.

The organization should define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how an organization manages services provided by external parties (see 5.21 and 5.22).

The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and the organization acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.

The organization should define:

- all relevant information security requirements associated with the use of the cloud services;
- cloud service selection criteria and scope of cloud service usage;
- roles and responsibilities related to the use and management of cloud services;
- which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer;
- how to obtain and utilize information security capabilities provided by the cloud service provider;
- how to obtain assurance on information security controls implemented by cloud service providers;
- how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers;
- procedures for handling information security incidents that occur in relation to the use of cloud services;
- its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;
- how to change or stop the use of cloud services including exit strategies for cloud services.

Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, the organization should review cloud service agreements with the cloud service provider(s). A cloud service agreement should address the confidentiality, integrity, availability and information handling requirements of the organization, with appropriate cloud service level objectives and cloud service qualitative objectives. The organization should also undertake relevant risk assessments to identify

the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the appropriate management of the organization.

An agreement between the cloud service provider and the organization, acting as the cloud service customer, should include the following provisions for the protection of the organization's data and availability of services:

- a) providing solutions based on industry accepted standards for architecture and infrastructure;
- b) managing access controls of the cloud service to meet the requirements of the organization;
- c) implementing malware monitoring and protection solutions;
- d) processing and storing the organization's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction;
- e) providing dedicated support in the event of an information security incident in the cloud service environment;
- f) ensuring that the organization's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted);
- g) supporting the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;
- h) providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service;
- i) providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the organization, acting as the cloud service customer;
- j) providing and returning information such as configuration files, source code and data that are owned by the organization, acting as the cloud service customer, when requested during the service provision or at termination of service.

The organization, acting as the cloud service customer, should consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to the organization, including:

- a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering;
- b) processing or storing information in a new geographical or legal jurisdiction;
- c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

The organization using cloud services should maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and the organization, acting as the cloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

Other information

This control considers cloud security from the perspective of the cloud service customer.

Additional information relating to cloud services can be found in ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 22123-1. Specifics related to cloud portability in support of exit strategies can be found in ISO/IEC 19941. Specifics related to information security and public cloud services are described in ISO/IEC 27017. Specifics related to PII protection in public clouds acting as PII processor are described

in ISO/IEC 27018. Supplier relationships for cloud services are covered by ISO/IEC 27036-4 and cloud service agreements and their contents are dealt with in the ISO/IEC 19086 series, with security and privacy specifically covered by ISO/IEC 19086-4.

5.24 Information security incident management planning and preparation

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

Control

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.

Guidance

Roles and responsibilities

The organization should establish appropriate information security incident management processes. Roles and responsibilities to carry out the incident management procedures should be determined and effectively communicated to the relevant internal and external interested parties.

The following should be considered:

- establishing a common method for reporting information security events including point of contact (see 6.8);
- establishing an incident management process to provide the organization with capability for managing information security incidents including administration, documentation, detection, triage, prioritization, analysis, communication and coordinating interested parties;
- establishing an incident response process to provide the organization with capability for assessing, responding to and learning from information security incidents;
- only allowing competent personnel to handle the issues related to information security incidents within the organization. Such personnel should be provided with procedure documentation and periodic training;
- establishing a process to identify required training, certification and ongoing professional development for incident response personnel.

Incident management procedures

The objectives for information security incident management should be agreed with management and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents including resolution time frame based on potential consequences and severity. Incident management procedures should be implemented to meet these objectives and priorities.

Management should ensure that an information security incident management plan is created considering different scenarios and procedures are developed and implemented for the following activities:

- a) evaluation of information security events according to criteria for what constitutes an information security incident;
- b) monitoring (see 8.15 and 8.16), detecting (see 8.16), classifying (see 5.25), analysing and reporting (see 6.8) of information security events and incidents (by human or automatic means);
- c) managing information security incidents to conclusion, including response and escalation (see 5.26), according to the type and the category of the incident, possible activation of crisis management and activation of continuity plans, controlled recovery from an incident and communication to internal and external interested parties;
- d) coordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers and clients (see 5.5 and 5.6);
- e) logging incident management activities;
- f) handling of evidence (see 5.28);
- g) root cause analysis or post-mortem procedures;
- h) identification of lessons learned and any improvements to the incident management procedures or information security controls in general that are required.

Reporting procedures

Reporting procedures should include:

- a) actions to be taken in case of an information security event (e.g. noting all pertinent details immediately such as malfunction occurring and messages on screen, immediately reporting to the point of contact and only taking coordinated actions);
- b) use of incident forms to support personnel to perform all necessary actions when reporting information security incidents;
- c) suitable feedback processes to ensure that those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed;
- d) creation of incident reports.

Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. breach notification requirements to regulators) should be considered when implementing incident management procedures.

Other information

Information security incidents can transcend organizational and national boundaries. To respond to such incidents, it is beneficial to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in the ISO/IEC 27035 series.

5.25 Assessment and decision on information security events

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose

To ensure effective categorization and prioritization of information security events.

Guidance

A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each information security event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

5.26 Response to information security incidents

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Control

Information security incidents should be responded to in accordance with the documented procedures.

Purpose

To ensure efficient and effective response to information security incidents.

Guidance

The organization should establish and communicate procedures on information security incident response to all relevant interested parties.

Information security incidents should be responded to by a designated team with the required competency (see 5.24).

The response should include the following:

- containing, if the consequences of the incident can spread, the systems affected by the incident;

- b) collecting evidence (see 5.28) as soon as possible after the occurrence;
- c) escalation, as required including crisis management activities and possibly invoking business continuity plans (see 5.29 and 5.30);
- d) ensuring that all involved response activities are properly logged for later analysis;
- e) communicating the existence of the information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle;
- f) coordinating with internal and external parties such as authorities, external interest groups and forums, suppliers and clients to improve response effectiveness and help to minimize consequences for other organizations;
- g) once the incident has been successfully addressed, formally closing and recording it;
- h) conducting information security forensic analysis, as required (see 5.28);
- i) performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (see 5.27);
- j) identifying and managing information security vulnerabilities and weaknesses including those related to controls which have caused, contributed to or failed to prevent the incident.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

5.27 Learning from information security incidents

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence

Control

Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

Purpose

To reduce the likelihood or consequences of future incidents.

Guidance

The organization should establish procedures to quantify and monitor the types, volumes and costs of information security incidents.

The information gained from the evaluation of information security incidents should be used to:

- a) enhance the incident management plan including incident scenarios and procedures (see 5.24);
- b) identify recurring or serious incidents and their causes to update the organization's information security risk assessment and determine and implement necessary additional controls to reduce the likelihood or consequences of future similar incidents. Mechanisms to enable that include collecting, quantifying and monitoring information about incident types, volumes and costs;
- c) enhance user awareness and training (see 6.3) by providing examples of what can happen, how to respond to such incidents and how to avoid them in the future.

Other information

The ISO/IEC 27035 series provides further guidance.

5.28 Collection of evidence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.

Guidance

Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of admission across the relevant jurisdictions.

In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off). Evidence typically needs to be collected in a manner that is admissible in the appropriate national courts of law or another disciplinary forum. It should be possible to show that:

- records are complete and have not been tampered with in any way;
- copies of electronic evidence are probably identical to the originals;
- any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Digital evidence can transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence.

Other information

When an information security event is first detected, it is not always obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve legal advice or law enforcement early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037 provides definitions and guidelines for identification, collection, acquisition and preservation of digital evidence.

The ISO/IEC 27050 series deals with electronic discovery, which involves the processing of electronically stored information as evidence.

5.29 Information security during disruption

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

Control

The organization should plan how to maintain information security at an appropriate level during disruption.

Purpose

To protect information and other associated assets during disruption.

Guidance

The organization should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity management processes.

Plans should be developed, implemented, tested, reviewed and evaluated to maintain or restore the security of information of critical business processes following interruption or failure. Security of information should be restored at the required level and in the required time frames.

The organization should implement and maintain:

- information security controls, supporting systems and tools within business continuity and ICT continuity plans;
- processes to maintain existing information security controls during disruption;
- compensating controls for information security controls that cannot be maintained during disruption.

Other information

In the context of business continuity and ICT continuity planning, it can be necessary to adapt the information security requirements depending on the type of disruption, compared to normal operational conditions. As part of the business impact analysis and risk assessment performed within business continuity management, the consequences of loss of confidentiality and integrity of information should be considered and prioritized in addition to the need for maintaining availability.

Information on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on business impact analysis (BIA) can be found in ISO/TS 22317.

5.30 ICT readiness for business continuity

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Continuity	#Resilience

Control

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

Guidance

ICT readiness for business continuity is an important component in business continuity management and information security management to ensure that the organization's objectives can continue to be met during disruption.

The ICT continuity requirements are the outcome of the business impact analysis (BIA). The BIA process should use impact types and criteria to assess the impacts over time resulting from the disruption of business activities that deliver products and services. The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). The BIA should then determine which resources are needed to support prioritized activities. An RTO should also be specified for these resources. A subset of these resources should include ICT services.

The BIA involving ICT services can be expanded to define performance and capacity requirements of ICT systems and recovery point objectives (RPO) of information required to support activities during disruption.

Based on the outputs from the BIA and risk assessment involving ICT services, the organization should identify and select ICT continuity strategies that consider options for before, during and after disruption. The business continuity strategies can comprise one or more solutions. Based on the strategies, plans should be developed, implemented and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

The organization should ensure that:

- a) an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence;
- b) ICT continuity plans, including response and recovery procedures detailing how the organization is planning to manage an ICT service disruption, are:
 - 1) regularly evaluated through exercises and tests;
 - 2) approved by management;
- c) ICT continuity plans include the following ICT continuity information:
 - 1) performance and capacity specifications to meet the business continuity requirements and objectives as specified in the BIA;
 - 2) RTO of each prioritized ICT service and the procedures for restoring those components;
 - 3) RPO of the prioritized ICT resources defined as information and the procedures for restoring the information.

Other information

Managing ICT continuity forms a key part of business continuity requirements concerning availability to be able to:

- a) respond and recover from disruption to ICT services regardless of the cause;
- b) ensure continuity of prioritized activities are supported by the required ICT services;
- c) respond before a disruption to ICT services occurs, and upon detection of at least one incident that can result in a disruption to ICT services.

Further guidance on ICT readiness for business continuity can be found in ISO/IEC 27031.

Further guidance on business continuity management systems can be found in ISO 22301 and ISO 22313.

Further guidance on BIA can be found in ISO/TS 22317.

5.31 Legal, statutory, regulatory and contractual requirements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection

Control

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

Guidance

General

External requirements including legal, statutory, regulatory or contractual requirements should be taken into consideration when:

- developing information security policies and procedures;
- designing, implementing or changing information security controls;
- classifying information and other associated assets as part of the process for setting information security requirements for internal needs or for supplier agreements;
- performing information security risk assessments and determining information security risk treatment activities;
- determining processes along with related roles and responsibilities relating to information security;
- determining suppliers' contractual requirements relevant to the organization and the scope of supply of products and services.

Legislation and regulations

The organization should:

- identify all legislation and regulations relevant to the organization's information security in order to be aware of the requirements for their type of business;
- take into consideration compliance in all relevant countries, if the organization:
 - conducts business in other countries;
 - uses products and services from other countries where laws and regulations can affect the organization;

- transfers information across jurisdictional borders where laws and regulations can affect the organization;
- c) review the identified legislation and regulation regularly in order to keep up to date with the changes and identify new legislation;
- d) define and document the specific processes and individual responsibilities to meet these requirements.

Cryptography

Cryptography is an area that often has specific legal requirements. Compliance with the relevant agreements, laws and regulations relating to the following items should be taken into consideration:

- a) restrictions on import or export of computer hardware and software for performing cryptographic functions;
- b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;
- c) restrictions on the usage of cryptography;
- d) mandatory or discretionary methods of access by the countries' authorities to encrypted information;
- e) validity of digital signatures, seals and certificates.

It is recommended to seek legal advice when ensuring compliance with relevant legislation and regulations, especially when encrypted information or cryptography tools are moved across jurisdictional borders.

Contracts

Contractual requirements related to information security should include those stated in:

- a) contracts with clients;
- b) contracts with suppliers (see 5.20);
- c) insurance contracts.

Other information

No other information.

5.32 Intellectual property rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem

Control

The organization should implement appropriate procedures to protect intellectual property rights.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

Guidance

The following guidelines should be considered to protect any material that can be considered intellectual property:

- a) defining and communicating a topic-specific policy on protection of intellectual property rights;
- b) publishing procedures for intellectual property rights compliance that define compliant use of software and information products;
- c) acquiring software only through known and reputable sources, to ensure that copyright is not infringed upon;
- d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;
- e) maintaining proof and evidence of ownership of licences, manuals, etc.;
- f) ensuring that any maximum number of users or resources [e.g. central processing units (CPUs)] permitted within the licence is not exceeded;
- g) carrying out reviews to ensure that only authorized software and licensed products are installed;
- h) providing procedures for maintaining appropriate licence conditions;
- i) providing procedures for disposing of or transferring software to others;
- j) complying with terms and conditions for software and information obtained from public networks and outside sources;
- k) not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law or the applicable licences;
- l) not copying, in full or in part, standards (e.g. ISO/IEC International Standards), books, articles, reports or other documents, other than permitted by copyright law or the applicable licences.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. See the ISO/IEC 19770 series for details about IT asset management.

Data can be acquired from outside sources. It is generally the case that such data is obtained under the terms of a data sharing agreement or similar legal instrument. Such data sharing agreements should make it clear what processing is permitted for the acquired data. It is also advisable that the provenance of the data is clearly stated. See ISO/IEC 23751 for details about data sharing agreements.

Legal, statutory, regulatory and contractual requirements can place restrictions on the copying of proprietary material. In particular, they can require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which can involve fines and criminal proceedings.

Aside from the organization needing to comply with its obligations towards third party intellectual property rights, the risks of personnel and third parties failing to uphold the organization's own intellectual property rights should also be managed.

5.33 Protection of records

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

Guidance

The organization should take the following steps to protect the authenticity, reliability, integrity and usability of records, as their business context and requirements for their management change over time:

- issue guidelines on the storage, handling chain of custody and disposal of records, which includes prevention of manipulation of records. These guidelines should be aligned with the organization's topic-specific policy on records management and other records requirements;
- draw up a retention schedule defining records and the period of time for which they should be retained.

The system of storage and handling should ensure identification of records and of their retention period taking into consideration national or regional legislation or regulations, as well as community or societal expectations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

When deciding on protection of specific organizational records, their corresponding information security classification, based on the organization's classification scheme, should be considered. Records should be categorized into record types (e.g. accounting records, business transaction records, personnel records, legal records), each with details of retention periods and type of allowable storage media which can be physical or electronic.

Data storage systems should be chosen such that required records can be retrieved in an acceptable time frame and format, depending on the requirements to be fulfilled.

Where electronic storage media are chosen, procedures to ensure the ability to access records (both storage media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be retained to enable decryption of the records for the length of time the records are retained (see 8.24).

Storage and handling procedures should be implemented in accordance with recommendations provided by manufacturers of storage media. Consideration should be given to the possibility of deterioration of media used for storage of records.

Other information

Records document individual events or transactions or can form aggregations that have been designed to document work processes, activities or functions. They are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a

record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business.

In the management of records, metadata is data describing the context, content and structure of records, as well as their management over time. Metadata is an essential component of any record.

It can be necessary to retain some records securely to meet legal, statutory, regulatory or contractual requirements, as well as to support essential business activities. National law or regulation can set the time period and data content for information retention. Further information about records management can be found in ISO 15489.

5.34 Privacy and protection of PII

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection

Control

The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

Guidance

The organization should establish and communicate a topic-specific policy on privacy and protection of PII to all relevant interested parties.

The organization should develop and implement procedures for the preservation of privacy and protection of PII. These procedures should be communicated to all relevant interested parties involved in the processing of personally identifiable information.

Compliance with these procedures and all relevant legislation and regulations concerning the preservation of privacy and protection of PII requires appropriate roles, responsibilities and controls. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to personnel, service providers and other interested parties on their individual responsibilities and the specific procedures that should be followed.

Responsibility for handling PII should be dealt with taking into consideration relevant legislation and regulations.

Appropriate technical and organizational measures to protect PII should be implemented.

Other information

A number of countries have introduced legislation placing controls on the collection, processing, transmission and deletion of PII. Depending on the respective national legislation, such controls can impose duties on those collecting, processing and disseminating PII and can also restrict the authority to transfer PII to other countries.

ISO/IEC 29100 provides a high-level framework for the protection of PII within ICT systems. Further information on privacy information management systems can be found in ISO/IEC 27701. Specific information regarding privacy information management for public clouds acting as PII processors can be found in ISO/IEC 27018.

ISO/IEC 29134 provides guidelines for privacy impact assessment (PIA) and gives an example of the structure and content of a PIA report. Compared with ISO/IEC 27005, this is focused on PII processing and relevant to those organizations that process PII. This can help identify privacy risks and possible mitigations to reduce these risks to acceptable levels.

5.35 Independent review of information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem

Control

The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.

Guidance

The organization should have processes to conduct independent reviews.

Management should plan and initiate periodic independent reviews. The reviews should include assessing opportunities for improvement and the need for changes to the approach to information security, including the information security policy, topic-specific policies and other controls.

Such reviews should be carried out by individuals independent of the area under review (e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews). Individuals carrying out these reviews should have the appropriate competence. The person conducting the reviews should not be in the line of authority to ensure they have the independence to make an assessment.

The results of the independent reviews should be reported to the management who initiated the reviews and, if appropriate, to top management. These records should be maintained.

If the independent reviews identify that the organization's approach and implementation to managing information security is inadequate [e.g. documented objectives and requirements are not met or are not compliant with the direction for information security stated in the information security policy and topic-specific policies (see 5.1)], management should initiate corrective actions.

In addition to the periodic independent reviews, the organization should consider conducting independent reviews when:

- laws and regulations which affect the organization change;
- significant incidents occur;
- the organization starts a new business or changes a current business;
- the organization starts to use a new product or service, or changes the use of a current product or service;
- the organization changes the information security controls and procedures significantly.

Normen-Download-Beuth-Heuteing Ktüm Lier-Wojtek PartGmbB-KdNr. 7791402-ID.rc251_5DuGlsklPuDu08_xSfMunqyNFN210K056r-2023-07-12 11:26:52

Other information

ISO/IEC 27007 and ISO/IEC TS 27008 provide guidance for carrying out independent reviews.

5.36 Compliance with policies, rules and standards for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem

Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

Guidance

Managers, service, product or information owners should identify how to review that information security requirements defined in the information security policy, topic-specific policies, rules, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

- a) identify the causes of the non-compliance;
- b) evaluate the need for corrective actions to achieve compliance;
- c) implement appropriate corrective actions;
- d) review corrective actions taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers, service, product or information owners should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see 5.35) when an independent review takes place in the area of their responsibility.

Corrective actions should be completed in a timely manner as appropriate to the risk. If not completed by the next scheduled review, progress should at least be addressed at that review.

Other information

Operational monitoring of system use is covered in 8.15, 8.16, 8.17.

5.37 Documented operating procedures

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Control

Operating procedures for information processing facilities should be documented and made available to personnel who need them.

Purpose

To ensure the correct and secure operation of information processing facilities.

Guidance

Documented procedures should be prepared for the organization's operational activities associated with information security, for example:

- when the activity needs to be performed in the same way by many people;
- when the activity is performed rarely and when next performed the procedure is likely to have been forgotten;
- when the activity is new and presents a risk if not performed correctly;
- prior to handing over the activity to new personnel.

The operating procedures should specify:

- the responsible individuals;
- the secure installation and configuration of systems;
- processing and handling of information, both automated and manual;
- backup (see 8.13) and resilience;
- scheduling requirements, including interdependencies with other systems;
- instructions for handling errors or other exceptional conditions [e.g. restrictions on the use of utility programs (see 8.18)], which can arise during job execution;
- support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
- storage media handling instructions (see 7.10 and 7.14);
- system restart and recovery procedures for use in the event of system failure;

- j) the management of audit trail and system log information (see 8.15 and 8.17) and video monitoring systems (see 7.4);
- k) monitoring procedures such as capacity, performance and security (see 8.6 and 8.16);
- l) maintenance instructions.

Documented operating procedures should be reviewed and updated when needed. Changes to documented operating procedures should be authorized. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

Other information

No other information.

6 People controls

6.1 Screening

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

Control

Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

Guidance

A screening process should be performed for all personnel including full-time, part-time and temporary staff. Where these individuals are contracted through suppliers of services, screening requirements should be included in the contractual agreements between the organization and the suppliers.

Information on all candidates being considered for positions within the organization should be collected and handled taking into consideration any appropriate legislation existing in the relevant jurisdiction. In some jurisdictions, the organization can be legally required to inform the candidates beforehand about the screening activities.

Verification should take into consideration all relevant privacy, PII protection and employment-based legislation and should, where permitted, include the following:

- a) availability of satisfactory references (e.g. business and personal references);
- b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity verification (e.g. passport or other acceptable document issued by appropriate authorities);

- e) more detailed verification, such as credit review or review of criminal records if the candidate takes on a critical role.

When an individual is hired for a specific information security role, the organization should make sure the candidate:

- a) has the necessary competence to perform the security role;
- b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities and, in particular, if these involve handling confidential information (e.g. financial information, personal information or health care information) the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews (e.g. who is eligible to screen people and how, when and why verification reviews are carried out).

In situations where verification cannot be completed in a timely manner, mitigating controls should be implemented until the review has been finished, for example:

- a) delayed onboarding;
- b) delayed deployment of corporate assets;
- c) onboarding with reduced access;
- d) termination of employment.

Verification checks should be repeated periodically to confirm ongoing suitability of personnel, depending on the criticality of a person's role.

Other information

No other information.

6.2 Terms and conditions of employment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control

The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.

Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered.

Guidance

The contractual obligations for personnel should take into consideration the organization's information security policy and relevant topic-specific policies. In addition, the following points can be clarified and stated:

- a) confidentiality or non-disclosure agreements that personnel who are given access to confidential information should sign prior to being given access to information and other associated assets (see 6.6);
- b) legal responsibilities and rights [e.g. regarding copyright laws or data protection legislation (see 5.32 and 5.34)];
- c) responsibilities for the classification of information and management of the organization's information and other associated assets, information processing facilities and information services handled by the personnel (see 5.9 to 5.13);
- d) responsibilities for the handling of information received from interested parties;
- e) actions to be taken if personnel disregard the organization's security requirements (see 6.4).

Information security roles and responsibilities should be communicated to candidates during the pre-employment process.

The organization should ensure that personnel agree to terms and conditions concerning information security. These terms and conditions should be appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The terms and conditions concerning information security should be reviewed when laws, regulations, the information security policy or topic-specific policies change.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 6.5).

Other information

A code of conduct can be used to state personnel's information security responsibilities regarding confidentiality, PII protection, ethics, appropriate use of the organization's information and other associated assets, as well as reputable practices expected by the organization.

An external party, with which supplier personnel are associated, can be required to enter into contractual agreements on behalf of the contracted individual.

If the organization is not a legal entity and does not have employees, the equivalent of contractual agreement and terms and conditions can be considered in line with the guidance of this control.

6.3 Information security awareness, education and training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem

Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

Guidance

General

An information security awareness, education and training programme should be established in line with the organization's information security policy, topic-specific policies and relevant procedures on information security, taking into consideration the organization's information to be protected and the information security controls that have been implemented to protect the information.

Information security awareness, education and training should take place periodically. Initial awareness, education and training can apply to new personnel and to those who transfer to new positions or roles with substantially different information security requirements.

Personnel's understanding should be assessed at the end of an awareness, education or training activity to test knowledge transfer and the effectiveness of the awareness, education and training programme.

Awareness

An information security awareness programme should aim to make personnel aware of their responsibilities for information security and the means by which those responsibilities are discharged.

The awareness programme should be planned taking into consideration the roles of personnel in the organization, including internal and external personnel (e.g. external consultants, supplier personnel). The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new personnel. It should also be built on lessons learnt from information security incidents.

The awareness programme should include a number of awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules and e-mails.

Information security awareness should cover general aspects such as:

- a) management's commitment to information security throughout the organization;
- b) familiarity and compliance needs concerning applicable information security rules and obligations, taking into account information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements;
- c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties;
- d) basic information security procedures [e.g. information security event reporting (6.8)] and baseline controls [e.g. password security (5.17)];
- e) contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

Education and training

The organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. Technical teams should have the skills for configuring and maintaining the required security level for devices, systems, applications and services. If there are missing skills, the organization should take action and acquire them.

The education and training programme should consider different forms [e.g. lectures or self-studies, being mentored by expert staff or consultants (on-the-job training), rotating staff members to follow different activities, recruiting already skilled people and hiring consultants]. It can use different means

of delivery including classroom-based, distance learning, web-based, self-paced and others. Technical personnel should keep their knowledge up to date by subscribing to newsletters and magazines or by attending conferences and events aimed at technical and professional improvement.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why', when possible. It is important that personnel understand the aim of information security and the potential effect, positive and negative, on the organization of their own behaviour.

Information security awareness, education and training can be part of, or conducted in collaboration with, other activities, for example general information management, ICT, security, privacy or safety training.

6.4 Disciplinary process

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem

Control

A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

Purpose

To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

Guidance

The disciplinary process should not be initiated without prior verification that an information security policy violation has occurred (see 5.28).

The formal disciplinary process should provide for a graduated response that takes into consideration factors such as:

- the nature (who, what, when, how) and gravity of the breach and its consequences;
- whether the offence was intentional (malicious) or unintentional (accidental);
- whether or not this is a first or repeated offence;
- whether or not the violator was properly trained.

The response should take into consideration relevant legal, statutory, regulatory contractual and business requirements as well as other factors as required. The disciplinary process should also be used as a deterrent to prevent personnel and other relevant interested parties from violating the information security policy, topic-specific policies and procedures for information security. Deliberate information security policy violations can require immediate actions.

Other information

Where possible, the identity of individuals subject to disciplinary action should be protected in line with applicable requirements.

When individuals demonstrate excellent behaviour with regard to information security, they can be rewarded to promote information security and encourage good behaviour.

6.5 Responsibilities after termination or change of employment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

Purpose

To protect the organization's interests as part of the process of changing or terminating employment or contracts.

Guidance

The process for managing termination or change of employment should define which information security responsibilities and duties should remain valid after termination or change. This can include confidentiality of information, intellectual property and other knowledge obtained, as well as responsibilities contained within any other confidentiality agreement (see 6.6). Responsibilities and duties still valid after termination of employment or contract should be contained in the individual's terms and conditions of employment (see 6.2), contract or agreement. Other contracts or agreements that continue for a defined period after the end of the individual's employment can also contain information security responsibilities.

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual.

A process should be established for the communication of the changes and of operating procedures to personnel, other interested parties and relevant contact persons (e.g. to customers and suppliers).

The process for the termination or change of employment should also be applied to external personnel (i.e. suppliers) when a termination occurs of personnel, the contract or the job with the organization, or when there is a change of the job within the organization.

Other information

In many organizations, the human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person transitioning to manage the information security aspects of the relevant procedures. In the case of personnel provided through an external party (e.g. through a supplier), this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

6.6 Confidentiality or non-disclosure agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Purpose

To maintain confidentiality of information accessible by personnel or external parties.

Guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to interested parties and personnel of the organization. Based on an organization's information security requirements, the terms in the agreements should be determined by taking into consideration the type of information that will be handled, its classification level, its use and the permissible access by the other party. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

- a) a definition of the information to be protected (e.g. confidential information);
- b) the expected duration of an agreement, including cases where it can be necessary to maintain confidentiality indefinitely or until the information becomes publicly available;
- c) the required actions when an agreement is terminated;
- d) the responsibilities and actions of signatories to avoid unauthorized information disclosure;
- e) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
- f) the permitted use of confidential information and rights of the signatory to use the information;
- g) the right to audit and monitor activities that involve confidential information for highly sensitive circumstances;
- h) the process for notification and reporting of unauthorized disclosure or confidential information leakage;
- i) the terms for information to be returned or destroyed at agreement termination;
- j) the expected actions to be taken in the case of non-compliance with the agreement.

The organization should take into consideration the compliance with confidentiality and non-disclosure agreements for the jurisdiction to which they apply (see 5.31, 5.32, 5.33, 5.34).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

Confidentiality and non-disclosure agreements protect the organization's information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

6.7 Remote working

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection

Control

Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

Purpose

To ensure the security of information when personnel are working remotely.

Guidance

Remote working occurs whenever personnel of the organization work from a location outside of the organization's premises, accessing information whether in hardcopy or electronically via ICT equipment. Remote working environments include those referred to as "teleworking", "telecommuting", "flexible workplace", "virtual work environments" and "remote maintenance".

NOTE It is possible that not all the recommendations in this guidance can be applied due to local legislation and regulations in different jurisdictions.

Organizations allowing remote working activities should issue a topic-specific policy on remote working that defines the relevant conditions and restrictions. Where deemed applicable, the following matters should be considered:

- the existing or proposed physical security of the remote working site, taking into account the physical security of the location and the local environment, including the different jurisdictions where personnel are located;
- rules and security mechanisms for the remote physical environment such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information and other associated assets, and information security event reporting (see 6.8);
- the expected physical remote working environments;
- the communications security requirements, taking into account the need for remote access to the organization's systems, the sensitivity of the information to be accessed and passed over the communication link and the sensitivity of the systems and applications;
- the use of remote access such as virtual desktop access that supports processing and storage of information on privately owned equipment;
- the threat of unauthorized access to information or resources from other persons at the remote working site (e.g. family and friends);
- the threat of unauthorized access to information or resources from other persons in public places;
- the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services;
- use of security measures, such as firewalls and protection against malware;

- j) secure mechanisms for deploying and initializing systems remotely;
- k) secure mechanisms for authentication and enablement of access privileges taking into consideration the vulnerability of single-factor authentication mechanisms where remote access to the organization's network is allowed.

The guidelines and measures to be considered should include:

- a) the provision of suitable equipment and storage furniture for the remote working activities, where the use of privately-owned equipment that is not under the control of the organization is not allowed;
- b) a definition of the work permitted, the classification of information that can be held and the internal systems and services that the remote worker is authorized to access;
- c) the provision of training for those working remotely and those providing support. This should include how to conduct business in a secure manner while working remotely;
- d) the provision of suitable communication equipment, including methods for securing remote access, such as requirements on device screen locks and inactivity timers; the enabling of device location tracking; installation of remote wipe capabilities;
- e) physical security;
- f) rules and guidance on family and visitor access to equipment and information;
- g) the provision of hardware and software support and maintenance;
- h) the provision of insurance;
- i) the procedures for backup and business continuity;
- j) audit and security monitoring;
- k) revocation of authority and access rights and the return of equipment when the remote working activities are terminated.

Other information

No other information.

6.8 Information security event reporting

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence

Control

The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

Purpose

To support timely, consistent and effective reporting of information security events that can be identified by personnel.

Guidance

All personnel and users should be made aware of their responsibility to report information security events as quickly as possible in order to prevent or minimize the effect of information security incidents.

They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. The reporting mechanism should be as easy, accessible and available as possible. Information security events include incidents, breaches and vulnerabilities.

Situations to be considered for information security event reporting include:

- a) ineffective information security controls;
- b) breach of information confidentiality, integrity or availability expectations;
- c) human errors;
- d) non-compliance with the information security policy, topic-specific policies or applicable standards;
- e) breaches of physical security measures;
- f) system changes that have not gone through the change management process;
- g) malfunctions or other anomalous system behaviour of software or hardware;
- h) access violations;
- i) vulnerabilities;
- j) suspected malware infection.

Personnel and users should be advised not to attempt to prove suspected information security vulnerabilities. Testing vulnerabilities can be interpreted as a potential misuse of the system and can also cause damage to the information system or service, and it can corrupt or obscure digital evidence. Ultimately, this can result in legal liability for the individual performing the testing.

Other information

See the ISO/IEC 27035 series for additional information.

7 Physical controls

7.1 Physical security perimeters

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Security perimeters should be defined and used to protect areas that contain information and other associated assets.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

Guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

- a) defining security perimeters and the siting and strength of each of the perimeters in accordance with the information security requirements related to the assets within the perimeter;

Normen-Download-Beuth-Heinking Kühn Lier-Wojtek PartGmbB-KdNr. 7791402-ID.rc251_5DuGlsklPuDu08_xSFmunqNFN210K056r-2023-07-12 11:26:52

- b) having physically sound perimeters for a building or site containing information processing facilities (i.e. there should be no gaps in the perimeter or areas where a break-in can easily occur). The exterior roofs, walls, ceilings and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms (e.g. bars, alarms, locks). Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level; ventilation points should also be considered;
- c) alarming, monitoring and testing all fire doors on a security perimeter in conjunction with the walls to establish the required level of resistance in accordance with suitable standards. They should operate in a failsafe manner.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities.

A secure area can be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access can be necessary between areas with different security requirements inside the security perimeter. The organization should consider having physical security measures that can be strengthened during increased threat situations.

7.2 Physical entry

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection

Control

Secure areas should be protected by appropriate entry controls and access points.

Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs.

Guidance

General

Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following guidelines should be considered:

- a) restricting access to sites and buildings to authorized personnel only. The process for the management of access rights to physical areas should include the provision, periodical review, update and revocation of authorizations (see 5.18);
- b) securely maintaining and monitoring a physical logbook or electronic audit trail of all access and protecting all logs (see 5.33) and sensitive authentication information;
- c) establishing and implementing a process and technical mechanisms for the management of access to areas where information is processed or stored. Authentication mechanisms include the use of access cards, biometrics or two-factor authentication such as an access card and secret PIN. Double security doors should be considered for access to sensitive areas;

- d) setting up a reception area monitored by personnel, or other means to control physical access to the site or building;
- e) inspecting and examining personal belongings of personnel and interested parties upon entry and exit;

NOTE Local legislation and regulations can exist regarding the possibility of inspecting personal belongings.

- f) requiring all personnel and interested parties to wear some form of visible identification and to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Easily distinguishable badges should be considered to better identify permanent employees, suppliers and visitors;
- g) granting supplier personnel restricted access to secure areas or information processing facilities only when required. This access should be authorized and monitored;
- h) giving special attention to physical access security in the case of buildings holding assets for multiple organizations;
- i) designing physical security measures so that they can be strengthened when the likelihood of physical incidents increases;
- j) securing other entry points such as emergency exits from unauthorized access;
- k) setting up a key management process to ensure the management of the physical keys or authentication information (e.g. lock codes, combination locks to offices, rooms and facilities such as key cabinets) and to ensure a log book or annual key audit and that access to physical keys or authentication information is controlled (see 5.17 for further guidance on authentication information).

Visitors

The following guidelines should be considered:

- a) authenticating the identity of visitors by an appropriate means;
- b) recording the date and time of entry and departure of visitors;
- c) only granting access for visitors for specific, authorized purposes and with instructions on the security requirements of the area and on emergency procedures;
- d) supervising all visitors, unless an explicit exception is granted.

Delivery and loading areas and incoming material

The following guidelines should be considered:

- a) restricting access to delivery and loading areas from outside of the building to identified and authorized personnel;
- b) designing the delivery and loading areas so that deliveries can be loaded and unloaded without delivery personnel gaining unauthorized access to other parts of the building;
- c) securing the external doors of delivery and loading areas when doors to restricted areas are opened;
- d) inspecting and examining incoming deliveries for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas;
- e) registering incoming deliveries in accordance with asset management procedures (see 5.9 and 7.10) on entry to the site;

- f) physically segregating incoming and outgoing shipments, where possible;
- g) inspecting incoming deliveries for evidence of tampering on the way. If tampering is discovered, it should be immediately reported to security personnel.

Other information

No other information.

7.3 Securing offices, rooms and facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Physical security for offices, rooms and facilities should be designed and implemented.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

Guidance

The following guidelines should be considered to secure offices, rooms and facilities:

- a) siting critical facilities to avoid access by the public;
- b) where applicable, ensuring buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;
- c) configuring facilities to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;
- d) not making directories, internal telephone books and online accessible maps identifying locations of confidential information processing facilities readily available to any unauthorized person.

Other information

No other information.

7.4 Physical security monitoring

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

Control

Premises should be continuously monitored for unauthorized physical access.

Purpose

To detect and deter unauthorized physical access.

Guidance

Physical premises should be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems should be continuously monitored to detect unauthorized access or suspicious behaviour by:

- a) installing video monitoring systems such as closed-circuit television to view and record access to sensitive areas within and outside an organization's premises;
- b) installing, according to relevant applicable standards, and periodically testing contact, sound or motion detectors to trigger an intruder alarm such as:
 - 1) installing contact detectors that trigger an alarm when a contact is made or broken in any place where a contact can be made or broken (such as windows and doors and underneath objects) to be used as a panic alarm;
 - 2) motion detectors based on infra-red technology which trigger an alarm when an object passes through their field of view;
 - 3) installing sensors sensitive to the sound of breaking glass which can be used to trigger an alarm to alert security personnel;
- c) using those alarms to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times; cover should also be provided for other areas (e.g. computer or communications rooms).

The design of monitoring systems should be kept confidential because disclosure can facilitate undetected break-ins.

Monitoring systems should be protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

The alarm system control panel should be placed in an alarmed zone and, for safety alarms, in a place that allows an easy exit route for the person who sets the alarm. The control panel and the detectors should have tamperproof mechanisms. The system should regularly be tested to ensure that it is working as intended, particularly if its components are battery powered.

Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

Other information

No other information.

7.5 Protecting against physical and environmental threats

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

Guidance

Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

Physical premises location and construction should take account of:

- a) local topography, such as appropriate elevation, bodies of water and tectonic fault lines;
- b) urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.

Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:

- a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);
- b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;
- c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;
- d) explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.

Other information

Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

7.6 Working in secure areas

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Security measures for working in secure areas should be designed and implemented.

Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

Guidance

The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

The following guidelines should be considered:

- a) making personnel aware only of the existence of, or activities within, a secure area on a need-to-know basis;
- b) avoiding unsupervised work in secure areas both for safety reasons and to reduce chances for malicious activities;
- c) physically locking and periodically inspecting vacant secure areas;
- d) not allowing photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized;
- e) appropriately controlling the carrying and use of user endpoint devices in secure areas;
- f) posting emergency procedures in a readily visible or accessible manner.

Other information

No other information.

7.7 Clear desk and clear screen

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

Guidance

The organization should establish and communicate a topic-specific policy on clear desk and clear screen to all relevant interested parties.

The following guidelines should be considered:

- a) locking away sensitive or critical business information (e.g. on paper or on electronic storage media) (ideally in a safe, cabinet or other form of security furniture) when not required, especially when the office is vacated;
- b) protecting user endpoint devices by key locks or other security means when not in use or unattended;

- c) leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature;
- d) making the originator collect outputs from printers or multi-function devices immediately. The use of printers with an authentication function, so the originators are the only ones who can get their printouts and only when standing next to the printer;
- e) securely storing documents and removable storage media containing sensitive information and, when no longer required, discarding them using secure disposal mechanisms;
- f) establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);
- g) clearing sensitive or critical information on whiteboards and other types of display when no longer required.

The organization should have procedures in place when vacating facilities including conducting a final sweep prior to leaving to ensure the organization's assets are not left behind (e.g. documents fallen behind drawers or furniture).

Other information

No other information.

7.8 Equipment siting and protection

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Equipment should be sited securely and protected.

Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

Guidance

The following guidelines should be considered to protect equipment:

- a) siting equipment to minimize unnecessary access into work areas and to avoid unauthorized access;
- b) carefully positioning information processing facilities handling sensitive data to reduce the risk of information being viewed by unauthorized persons during their use;
- c) adopting controls to minimize the risk of potential physical and environmental threats [e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism];
- d) establishing guidelines for eating, drinking and smoking in proximity to information processing facilities;
- e) monitoring environmental conditions, such as temperature and humidity, for conditions which can adversely affect the operation of information processing facilities;

- f) applying lightning protection to all buildings and fitting lightning protection filters to all incoming power and communications lines;
- g) considering the use of special protection methods, such as keyboard membranes, for equipment in industrial environments;
- h) protecting equipment processing confidential information to minimize the risk of information leakage due to electromagnetic emanation;
- i) physically separating information processing facilities managed by the organization from those not managed by the organization.

Other information

No other information.

7.9 Security of assets off-premises

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Off-site assets should be protected.

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

Guidance

Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization [bring your own device (BYOD)] needs protection. The use of these devices should be authorized by management.

The following guidelines should be considered for the protection of devices which store or process information outside the organization's premises:

- a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;
- b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);
- c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to be transferred with the asset should be securely deleted before the transfer;
- d) where necessary and practical, requiring authorization for equipment and media to be removed from the organization's premises and keeping a record of such removals in order to maintain an audit trail (see 5.14);
- e) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing;
- f) implementing location tracking and ability for remote wiping of devices.

Permanent installation of equipment outside the organization's premises [such as antennas and automated teller machines (ATMs)] can be subject to higher risk of damage, theft or eavesdropping. These risks can vary considerably between locations and should be taken into account in determining the most appropriate measures. The following guidelines should be considered when siting this equipment outside of the organization's premises:

- a) physical security monitoring (see 7.4);
- b) protecting against physical and environmental threats (see 7.5);
- c) physical access and tamper proofing controls;
- d) logical access controls.

Other information

More information about other aspects of protecting information storing and processing equipment and user endpoint devices can be found in 8.1 and 6.7.

7.10 Storage media

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

Guidance

Removable storage media

The following guidelines for the management of removable storage media should be considered:

- a) establishing a topic-specific policy on the management of removable storage media and communicating such topic-specific policy to anyone who uses or handles removable storage media;
- b) where necessary and practical, requiring authorization for storage media to be removed from the organization and keeping a record of such removals in order to maintain an audit trail;
- c) storing all storage media in a safe, secure environment according to their information classification and protecting them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications;
- d) if information confidentiality or integrity are important considerations, using cryptographic techniques to protect information on removable storage media;
- e) to mitigate the risk of storage media degrading while stored information is still needed, transferring the information to fresh storage media before becoming unreadable;
- f) storing multiple copies of valuable information on separate storage media to further reduce the risk of coincidental information damage or loss;

- g) considering the registration of removable storage media to limit the chance for information loss;
- h) only enabling removable storage media ports [e.g. secure digital (SD) card slots and universal serial bus (USB) ports] if there is an organizational reason for their use;
- i) where there is a need to use removable storage media, monitoring the transfer of information to such storage media;
- j) information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.

In this control, media includes paper documents. When transferring physical storage media, apply security measures in 5.14.

Secure reuse or disposal

Procedures for the secure reuse or disposal of storage media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

- a) if storage media containing confidential information need to be reused within the organization, securely deleting data or formatting the storage media before reuse (see 8.10);
- b) disposing of storage media containing confidential information securely when not needed anymore (e.g. by destroying, shredding or securely deleting the content);
- c) having procedures in place to identify the items that can require secure disposal;
- d) many organizations offer collection and disposal services for storage media. Care should be taken in selecting a suitable external party supplier with adequate controls and experience;
- e) logging the disposal of sensitive items in order to maintain an audit trail;
- f) when accumulating storage media for disposal, giving consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

A risk assessment should be performed on damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 7.14).

Other information

When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

7.11 Supporting utilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Control

Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

Guidance

Organizations depend on utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) to support their information processing facilities. Therefore, the organization should:

- a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;
- b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
- c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;
- d) if necessary, raise alarms to detect utilities malfunctions;
- e) if necessary, ensure utilities have multiple feeds with diverse physical routing;
- f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;
- g) ensure equipment supporting the utilities is connected to the internet only when needed and only in a secure manner.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. Emergency contact details should be recorded and available to personnel in the event of an outage.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

7.12 Cabling security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

Control

Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

Guidance

The following guidelines for cabling security should be considered:

- a) power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, such as floor cable protector and utility pole; if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);
- b) segregating power cables from communications cables to prevent interference;

- c) for sensitive or critical systems, further controls to consider include:
 - 1) installation of armoured conduit and locked rooms or boxes and alarms at inspection and termination points;
 - 2) use of electromagnetic shielding to protect the cables;
 - 3) periodical technical sweeps and physical inspections to detect unauthorized devices being attached to the cables;
 - 4) controlled access to patch panels and cable rooms (e.g. with mechanical keys or PINs);
 - 5) use of fibre-optic cables;
- d) labelling cables at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Specialist advice should be sought on how to manage risks arising from cabling incidents or malfunctions.

Other information

Sometimes power and telecommunications cabling are shared resources for more than one organization occupying co-located premises.

7.13 Equipment maintenance

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

Control

Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

Guidance

The following guidelines for equipment maintenance should be considered:

- a) maintaining equipment in accordance with the supplier's recommended service frequency and specifications;
- b) implementing and monitoring of a maintenance programme by the organization;
- c) only authorized maintenance personnel carrying out repairs and maintenance on equipment;
- d) keeping records of all suspected or actual faults, and of all preventive and corrective maintenance;
- e) implementing appropriate controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; subjecting the maintenance personnel to a suitable confidentiality agreement;
- f) supervising maintenance personnel when carrying out maintenance on site;
- g) authorizing and controlling access for remote maintenance;

- h) applying security measures for assets off-premises (see 7.9) if equipment containing information is taken off premises for maintenance;
- i) complying with all maintenance requirements imposed by insurance;
- j) before putting equipment back into operation after maintenance, inspecting it to ensure that the equipment has not been tampered with and is functioning properly;
- k) applying measures for secure disposal or re-use of equipment (see 7.14) if it is determined that equipment is to be disposed of.

Other information

Equipment includes technical components of information processing facilities, uninterruptible power supply (UPS) and batteries, power generators, power alternators and converters, physical intrusion detection systems and alarms, smoke detectors, fire extinguishers, air conditioning and lifts.

7.14 Secure disposal or re-use of equipment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

Control

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose

To prevent leakage of information from equipment to be disposed or re-used.

Guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function. See 7.10 for detailed guidance on secure disposal of storage media and 8.10 for guidance on information deletion.

Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

The organization should consider the removal of security controls such as access controls or surveillance equipment at the end of lease or when moving out of premises. This depends on factors such as:

- a) its lease agreement to return the facility to original condition;
- b) minimizing the risk of leaving systems with sensitive information on them for the next tenant (e.g. user access lists, video or image files);
- c) the ability to reuse the controls at the next facility.

Other information

Damaged equipment containing storage media can require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

- a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files);
- b) the cryptographic keys are long enough to resist brute force attacks;
- c) the cryptographic keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on cryptography, see 8.24.

Techniques for securely overwriting storage media differ according to the storage media technology and the classification level of the information on the storage media. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

See ISO/IEC 27040 for detail on methods for sanitizing storage media.

8 Technological controls

8.1 User endpoint devices

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

Information stored on, processed by or accessible via user endpoint devices should be protected.

Purpose

To protect information against the risks introduced by using user endpoint devices.

Guidance

General

The organization should establish a topic-specific policy on secure configuration and handling of user endpoint devices. The topic-specific policy should be communicated to all relevant personnel and consider the following:

- a) the type of information and the classification level that the user endpoint devices can handle, process, store or support;
- b) registration of user endpoint devices;
- c) requirements for physical protection;
- d) restriction of software installation (e.g. remotely controlled by system administrators);
- e) requirements for user endpoint device software (including software versions) and for applying updates (e.g. active automatic updating);
- f) rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);
- g) access controls;
- h) storage device encryption;

- i) protection against malware;
- j) remote disabling, deletion or logout;
- k) backups;
- l) usage of web services and web applications;
- m) end user behaviour analytics (see 8.16);
- n) the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g. USB ports);
- o) the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organization's information and other associated assets (e.g. software) from other information and other associated assets on the device.

Consideration should be given as to whether certain information is so sensitive that it can only be accessed via user endpoint devices, but not stored on such devices. In such cases, additional technical safeguards can be required on the device. For example, ensuring that downloading files for offline working is disabled and that local storage such as SD card is disabled.

As far as possible, the recommendations on this control should be enforced through configuration management (see 8.9) or automated tools.

User responsibility

All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures. Users should be advised to:

- a) log-off active sessions and terminate services when no longer needed;
- b) protect user endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use; not leave devices carrying important, sensitive or critical business information unattended;
- c) use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);
- d) physically protect user endpoint devices against theft (e.g. in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure taking into account legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organization should be established for cases of theft or loss of user endpoint devices.

Use of personal devices

Where the organization allows the use of personal devices (sometimes known as BYOD), in addition to the guidance given in this control, the following should be considered:

- a) separation of personal and business use of the devices, including using software to support such separation and protect business data on a private device;
- b) providing access to business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. In such cases, PII protection legislation should be considered;
- c) topic-specific policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

- d) access to privately owned equipment (to verify the security of the machine or during an investigation), which can be prevented by legislation;
- e) software licensing agreements that are such that organizations can become liable for licensing for client software on user endpoint devices owned privately by personnel or external party users.

Wireless connections

The organization should establish procedures for:

- a) the configuration of wireless connections on devices (e.g. disabling vulnerable protocols);
- b) using wireless or wired connections with appropriate bandwidth in accordance with relevant topic-specific policies (e.g. because backups or software updates are needed).

Other information

Controls to protect information on user endpoint devices depend on whether the user endpoint device is used only inside of the organization's secured premises and network connections, or whether it is exposed to increased physical and network related threats outside of the organization.

The wireless connections for user endpoint devices are similar to other types of network connections but have important differences that should be considered when identifying controls. In particular, back-up of information stored on user endpoint devices can sometimes fail because of limited network bandwidth or because user endpoint devices are not connected at the times when backups are scheduled.

For some USB ports, such as USB-C, disabling the USB port is not possible because it is used for other purposes (e.g. power delivery and display output).

8.2 Privileged access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

The allocation and use of privileged access rights should be restricted and managed.

Purpose

To ensure only authorized users, software components and services are provided with privileged access rights.

Guidance

The allocation of privileged access rights should be controlled through an authorization process in accordance with the relevant topic-specific policy on access control (see 5.15). The following should be considered:

- a) identifying users who need privileged access rights for each system or process (e.g. operating systems, database management systems and applications);
- b) allocating privileged access rights to users as needed and on an event-by-event basis in line with the topic-specific policy on access control (see 5.15) (i.e. only to individuals with the necessary competence to carry out activities that require privileged access and based on the minimum requirement for their functional roles);

- c) maintaining an authorization process (i.e. determining who can approve privileged access rights, or not granting privileged access rights until the authorization process is complete) and a record of all privileges allocated;
- d) defining and implementing requirements for expiry of privileged access rights;
- e) taking measures to ensure that users are aware of their privileged access rights and when they are in privileged access mode. Possible measures include using specific user identities, user interface settings or even specific equipment;
- f) authentication requirements for privileged access rights can be higher than the requirements for normal access rights. Re-authentication or authentication step-up can be necessary before doing work with privileged access rights;
- g) regularly, and after any organizational change, reviewing users working with privileged access rights in order to verify if their duties, roles, responsibilities and competence still qualify them for working with privileged access rights (see 5.18);
- h) establishing specific rules in order to avoid the use of generic administration user IDs (such as “root”), depending on systems’ configuration capabilities. Managing and protecting authentication information of such identities (see 5.17);
- i) granting temporary privileged access just for the time window necessary to implement approved changes or activities (e.g. for maintenance activities or some critical changes), rather than permanently granting privileged access rights. This is often referred as break glass procedure, and often automated by privilege access management technologies;
- j) logging all privileged access to systems for audit purposes;
- k) not sharing or linking identities with privileged access rights to multiple persons, assigning each person a separate identity which allows assigning specific privileged access rights. Identities can be grouped (e.g. by defining an administrator group) in order to simplify the management of privileged access rights;
- l) only using identities with privileged access rights for undertaking administrative tasks and not for day-to-day general tasks [i.e. checking email, accessing the web (users should have a separate normal network identity for these activities)].

Other information

Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.

Inappropriate use of system administrator privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

More information related to access management and the secure management of access to information and information and communications technologies resources can be found in ISO/IEC 29146.

8.3 Information access restriction

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

Purpose

To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

Guidance

Access to information and other associated assets should be restricted in accordance with the established topic-specific policies. The following should be considered in order to support access restriction requirements:

- a) not allowing access to sensitive information by unknown user identities or anonymously. Public or anonymous access should only be granted to storage locations that do not contain any sensitive information;
- b) providing configuration mechanisms to control access to information in systems, applications and services;
- c) controlling which data can be accessed by a particular user;
- d) controlling which identities or group of identities have which access, such as read, write, delete and execute;
- e) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

Further, dynamic access management techniques and processes to protect sensitive information that has high value to the organization should be considered when the organization:

- a) needs granular control over who can access such information during what period and in what way;
- b) wants to share such information with people outside the organization and maintain control over who can access it;
- c) wants to dynamically manage, in real-time, the use and distribution of such information;
- d) wants to protect such information against unauthorized changes, copying and distribution (including printing);
- e) wants to monitor the use of the information;
- f) wants to record any changes to such information that take place in case a future investigation is required.

Dynamic access management techniques should protect information throughout its life cycle (i.e. creation, processing, storage, transmission and disposal), including:

- a) establishing rules on the management of dynamic access based on specific use cases considering:
 - 1) granting access permissions based on identity, device, location or application;
 - 2) leveraging the classification scheme in order to determine what information needs to be protected with dynamic access management techniques;
- b) establishing operational, monitoring and reporting processes and supporting technical infrastructure.

Normen-Download-Beuth-Heinking Ktüm Lier-Wojtek PartGmbB-KdNr. 7791402-ID.rc25i_5DuGlsklPuDu08_xSfMunqvNFN210K056r-2023-07-12 11:26:52

Dynamic access management systems should protect information by:

- a) requiring authentication, appropriate credentials or a certificate to access information;
- b) restricting access, for example to a specified time frame (e.g. after a given date or until a particular date);
- c) using encryption to protect information;
- d) defining the printing permissions for the information;
- e) recording who accesses the information and how the information is used;
- f) raising alerts if attempts to misuse the information are detected.

Other information

Dynamic access management techniques and other dynamic information protection technologies can support the protection of information even when data is shared beyond the originating organization, where traditional access controls cannot be enforced. It can be applied to documents, emails or other files containing information to limit who can access the content and in what way. It can be at a granular level and be adapted over the life cycle of the information.

Dynamic access management techniques do not replace classical access management [e.g. using access control lists (ACLs)], but can add more factors for conditionality, real-time evaluation, just-in-time data reduction and other enhancements that can be useful for the most sensitive information. It offers a way to control access outside the organization's environment. Incident response can be supported by dynamic access management techniques as permissions can be modified or revoked at any time.

Additional information on a framework for access management is provided in ISO/IEC 29146.

8.4 Access to source code

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection

Control

Read and write access to source code, development tools and software libraries should be appropriately managed.

Purpose

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.

Guidance

Access to source code and associated items (such as designs, specifications, verification plans and validation plans) and development tools (e.g. compilers, builders, integration tools, test platforms and environments) should be strictly controlled.

For source code, this can be achieved by controlling central storage of such code, preferably in source code management system.

Read access and write access to source code can differ based on the personnel's role. For example, read access to source code can be broadly provided inside the organization, but write access to source code

is only made available to privileged personnel or designated owners. Where code components are used by several developers within an organization, read access to a centralized code repository should be implemented. Furthermore, if open-source code or third-party code components are used inside an organization, read access to such external code repositories can be broadly provided. However, write access should still be restricted.

The following guidelines should be considered to control access to program source libraries in order to reduce the potential for corruption of computer programs:

- a) managing the access to program source code and the program source libraries according to established procedures;
- b) granting read and write access to source code based on business needs and managed to address risks of alteration or misuse and according to established procedures;
- c) updating of source code and associated items and granting of access to source code in accordance with change control procedures (see 8.32) and only performing it after appropriate authorization has been received;
- d) not granting developers direct access to the source code repository, but through developer tools that control activities and authorizations on the source code;
- e) holding program listings in a secure environment, where read and write access should be appropriately managed and assigned;
- f) maintaining an audit log of all accesses and of all changes to source code.

If the program source code is intended to be published, additional controls to provide assurance on its integrity (e.g. digital signature) should be considered.

Other information

If access to source code is not properly controlled, source code can be modified or some data in the development environment (e.g. copies of production data, configuration details) can be retrieved by unauthorized persons.

8.5 Secure authentication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

Guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

The strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods

alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used.

Authentication information should be accompanied by additional authentication factors for accessing critical information systems (also known as multi-factor authentication). Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorized accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

Biometric authentication information should be invalidated if it is ever compromised. Biometric authentication can be unavailable depending on the conditions of use (e.g. moisture or aging). To prepare for these issues, biometric authentication should be accompanied with at least one alternative authentication technique.

The procedure for logging into a system or application should be designed to minimize the risk of unauthorized access. Log-on procedures and technologies should be implemented considering the following:

- a) not displaying sensitive system or application information until the log-on process has been successfully completed in order to avoid providing an unauthorized user with any unnecessary assistance;
- b) displaying a general notice warning that the system or the application or the service should only be accessed by authorized users;
- c) not providing help messages during the log-on procedure that would aid an unauthorized user (e.g. if an error condition arises, the system should not indicate which part of the data is correct or incorrect);
- d) validating the log-on information only on completion of all input data;
- e) protecting against brute force log-on attempts on usernames and passwords [e.g. using completely automated public Turing test to tell computers and humans apart (CAPTCHA), requiring password reset after a predefined number of failed attempts or blocking the user after a maximum number of errors];
- f) logging unsuccessful and successful attempts;
- g) raising a security event if a potential attempted or successful breach of log-on controls is detected (e.g. sending an alert to the user and the organization's system administrators when a certain number of wrong password attempts has been reached);
- h) displaying or sending the following information on a separate channel on completion of a successful log-on:
 - 1) date and time of the previous successful log-on;
 - 2) details of any unsuccessful log-on attempts since the last successful log-on;
- i) not displaying a password in clear text when it is being entered; in some cases, it can be required to de-activate this functionality in order to facilitate user log-on (e.g. for accessibility reasons or to avoid blocking users because of repeated errors);
- j) not transmitting passwords in clear text over a network to avoid being captured by a network "sniffer" program;
- k) terminating inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on user endpoint devices;

- l) restricting connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information

Additional information on entity authentication assurance can be found in ISO/IEC 29115.

8.6 Capacity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_ Ecosystem #Protection

Control

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

Purpose

To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

Guidance

Capacity requirements for information processing facilities, human resources, offices and other facilities should be identified, taking into account the business criticality of the concerned systems and processes.

System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems.

The organization should perform stress-tests of systems and services to confirm that sufficient system capacity is available to meet peak performance requirements.

Detective controls should be put in place to indicate problems in due time.

Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention should be paid to any resources with long procurement lead times or high costs. Therefore, managers, service or product owners should monitor the utilization of key system resources.

Managers should use capacity information to identify and avoid potential resource limitations and dependency on key personnel which can present a threat to system security or services and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. The following should be considered to increase capacity:

- hiring new personnel;
- obtaining new facilities or space;
- acquiring more powerful processing systems, memory and storage;
- making use of cloud computing, which has inherent characteristics that directly address issues of capacity. Cloud computing has elasticity and scalability which enable on-demand rapid expansion and reduction in resources available to particular applications and services.

The following should be considered to reduce demand on the organization's resources:

- a) deletion of obsolete data (disk space);
- b) disposal of hardcopy records that have met their retention period (free up shelving space);
- c) decommissioning of applications, systems, databases or environments;
- d) optimizing batch processes and schedules;
- e) optimizing application code or database queries;
- f) denying or restricting bandwidth for resource-consuming services if these are not critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

For more detail on the elasticity and scalability of cloud computing, see ISO/IEC TS 23167.

8.7 Protection against malware

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

Control

Protection against malware should be implemented and supported by appropriate user awareness.

Purpose

To ensure information and other associated assets are protected against malware.

Guidance

Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls. Use of malware detection and repair software alone is not usually adequate. The following guidance should be considered:

- a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)] (see 8.19 and 8.32);
- b) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting);
- c) reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management (see 8.8 and 8.19)];
- d) conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved files or unauthorized amendments;
- e) establishing protective measures against risks associated with obtaining files and software either from or via external networks or on any other medium;

- f) installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:
 - 1) scanning any data received over networks or via any form of electronic storage media, for malware before use;
 - 2) scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization;
 - 3) scanning webpages for malware when accessed;
- g) determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:
 - 1) defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices and servers;
 - 2) the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;
- h) taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;
- i) implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date. This can be necessary when the protection against malware causes disruption to normal operations;
- j) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery measures (see 8.13);
- k) isolating environments where catastrophic consequences can occur;
- l) defining procedures and responsibilities to deal with protection against malware on systems, including training in their use, reporting and recovering from malware attacks;
- m) providing awareness or training (see 6.3) to all users on how to identify and potentially mitigate the receipt, sending or installation of malware infected emails, files or programs [the information collected in n) and o) can be used to ensure awareness and training are kept up-to-date];
- n) implementing procedures to regularly collect information about new malware, such as subscribing to mailing lists or reviewing relevant websites;
- o) verifying that information relating to malware, such as warning bulletins, comes from qualified and reputable sources (e.g. reliable internet sites or suppliers of malware detection software) and is accurate and informative.

Other information

It is not always possible to install software that protects against malware on some systems (e.g. some industrial control systems). Some forms of malware infect computer operating systems and computer firmware such that common malware controls cannot clean the system and a full reimaging of the operating system software and sometimes the computer firmware is necessary to return to a secure state.

8.8 Management of technical vulnerabilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_vulnerability_management	#Governance_and_Ecosystem #Protection #Defence

Control

Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

Purpose

To prevent exploitation of technical vulnerabilities.

Guidance

Identifying technical vulnerabilities

The organization should have an accurate inventory of assets (see 5.9 to 5.14) as a prerequisite for effective technical vulnerability management; the inventory should include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

To identify technical vulnerabilities, the organization should consider:

- defining and establishing the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, updating, asset tracking and any coordination responsibilities required;
- for software and other technologies (based on the asset inventory list, see 5.9), identifying information resources that will be used for identifying relevant technical vulnerabilities and maintaining awareness about them. Updating the list of information resources based on changes in the inventory or when other new or useful resources are found;
- requiring suppliers of information system (including their components) to ensure vulnerability reporting, handling and disclosure, including the requirements in applicable contracts (see 5.20);
- using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;
- conducting planned, documented and repeatable penetration tests or vulnerability assessments by competent and authorized persons to support the identification of vulnerabilities. Exercising caution as such activities can lead to a compromise of the security of the system;
- tracking the usage of third-party libraries and source code for vulnerabilities. This should be included in secure coding (see 8.28).

The organization should develop procedures and capabilities to:

- detect the existence of vulnerabilities in its products and services including any external component used in these;
- receive vulnerability reports from internal or external sources.

The organization should provide a public point of contact as part of a topic-specific policy on vulnerability disclosure so that researchers and others are able to report issues. The organization should establish vulnerability reporting procedures, online reporting forms and making use of appropriate threat intelligence or information sharing forums. The organization should also consider bug bounty programs

where rewards are offered as an incentive to assist organizations in identifying vulnerabilities in order to appropriately remediate them. The organization should also share information with competent industry bodies or other interested parties.

Evaluating technical vulnerabilities

To evaluate identified technical vulnerabilities, the following guidance should be considered:

- a) analyse and verify reports to determine what response and remediation activity is needed;
- b) once a potential technical vulnerability has been identified, identifying the associated risks and the actions to be taken. Such actions can involve updating vulnerable systems or applying other controls.

Taking appropriate measures to address technical vulnerabilities

A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. If changes are necessary, the original software should be retained and the changes applied to a designated copy. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

The following guidance should be considered to address technical vulnerabilities:

- a) taking appropriate and timely action in response to the identification of potential technical vulnerabilities; defining a timeline to react to notifications of potentially relevant technical vulnerabilities;
- b) depending on how urgently a technical vulnerability needs to be addressed, carrying out the action according to the controls related to change management (see 8.32) or by following information security incident response procedures (see 5.26);
- c) only using updates from legitimate sources (which can be internal or external to the organization);
- d) testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated [i.e. if an update is available, assessing the risks associated with installing the update (the risks posed by the vulnerability should be compared with the risk of installing the update)];
- e) addressing systems at high risk first;
- f) develop remediation (typically software updates or patches);
- g) test to confirm if the remediation or mitigation is effective;
- h) provide mechanisms to verify the authenticity of remediation;
- i) if no update is available or the update cannot be installed, considering other controls, such as:
 - 1) applying any workaround suggested by the software vendor or other relevant sources;
 - 2) turning off services or capabilities related to the vulnerability;
 - 3) adapting or adding access controls (e.g. firewalls) at network borders (see 8.20 to 8.22);
 - 4) shielding vulnerable systems, devices or applications from attack through deployment of suitable traffic filters (sometimes called virtual patching);
 - 5) increasing monitoring to detect actual attacks;
 - 6) raising awareness of the vulnerability.

For acquired software, if the vendors regularly release information about security updates for their software and provide a facility to install such updates automatically, the organization should decide whether to use the automatic update or not.

Other considerations

An audit log should be kept for all steps undertaken in technical vulnerability management.

The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out in case an incident occurs.

Where the organization uses a cloud service supplied by a third-party cloud service provider, technical vulnerability management of cloud service provider resources should be ensured by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management should be part of the cloud service agreement and this should include processes for reporting the cloud service provider's actions relating to technical vulnerabilities (see 5.23). For some cloud services, there are respective responsibilities for the cloud service provider and the cloud service customer. For example, the cloud service customer is responsible for vulnerability management of its own assets used for the cloud services.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 8.32).

There is a possibility that an update does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling an update cannot be easily achieved once the update has been applied.

If adequate testing of the updates is not possible (e.g. because of costs or lack of resources) a delay in updating can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031 can be beneficial.

Where software patches or updates are produced, the organization can consider providing an automated update process where these updates are installed on affected systems or products without the need for intervention by the customer or the user. If an automated update process is offered, it can allow the customer or user to choose an option to turn off the automatic update or control the timing of the installation of the update.

Where the vendor provides an automated update process and the updates can be installed on affected systems or products without the need for intervention, the organization determines if it applies the automated process or not. One reason for not electing for automated update is to retain control over when the update is performed. For example, a software used for a business operation cannot be updated until the operation has completed.

A weakness with vulnerability scanning is that it is possible it does not fully account for defence in depth: two countermeasures that are always invoked in sequence can have vulnerabilities that are masked by strengths in the other. The composite countermeasure is not vulnerable, whereas a vulnerability scanner can report that both components are vulnerable. The organization should therefore take care in reviewing and acting on vulnerability reports.

Many organizations supply software, systems, products and services not only within the organization but also to interested parties such as customers, partners or other users. These software, systems, products and services can have information security vulnerabilities that affect the security of users.

Organizations can release remediation and disclose information about vulnerabilities to users (typically through a public advisory) and provide appropriate information for software vulnerability database services.

For more information relating to the management of technical vulnerabilities when using cloud computing, see the ISO/IEC 19086 series and ISO/IEC 27017.

ISO/IEC 29147 provides detailed information on receiving vulnerability reports and publishing vulnerability advisories. ISO/IEC 30111 provides detailed information about handling and resolving reported vulnerabilities.

8.9 Configuration management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

Guidance

General

The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Roles, responsibilities and procedures should be in place to ensure satisfactory control of all configuration changes.

Standard templates

Standard templates for the secure configuration of hardware, software, services and networks should be defined:

- using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations);
- considering the level of protection needed in order to determine a sufficient level of security;
- supporting the organization's information security policy, topic-specific policies, standards and other security requirements;
- considering the feasibility and applicability of security configurations in the organization's context.

The templates should be reviewed periodically and updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced.

The following should be considered for establishing standard templates for the secure configuration of hardware, software, services and networks:

- minimizing the number of identities with privileged or administrator level access rights;

- b) disabling unnecessary, unused or insecure identities;
- c) disabling or restricting unnecessary functions and services;
- d) restricting access to powerful utility programs and host parameter settings;
- e) synchronizing clocks;
- f) changing vendor default authentication information such as default passwords immediately after installation and reviewing other important default security-related parameters;
- g) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity;
- h) verifying that licence requirements have been met (see 5.32).

Managing configurations

Established configurations of hardware, software, services and networks should be recorded and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

Configuration records can contain as relevant:

- a) up-to-date owner or point of contact information for the asset;
- b) date of the last change of configuration;
- c) version of configuration template;
- d) relation to configurations of other assets.

Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Other information

Documentation for systems often records details about the configuration of both hardware and software.

System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling.

Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).

Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

8.10 Information deletion

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

Control

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

Guidance

General

Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.

When deleting information on systems, applications and services, the following should be considered:

- selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations;
- recording the results of deletion as evidence;
- when using service suppliers of information deletion, obtaining evidence of information deletion from them.

Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

Deletion methods

In accordance with the organization's topic-specific policy on data retention and taking into consideration relevant legislation and regulations, sensitive information should be deleted when no longer required, by:

- configuring systems to securely destroy information when no longer required (e.g. after a defined period subject to the topic-specific policy on data retention or by subject access request);
- deleting obsolete versions, copies and temporary files wherever they are located;
- using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools;
- using approved, certified providers of secure disposal services;
- using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives and other magnetic storage media).

Where cloud services are used, the organization should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, the organization should use it, or request that the cloud service provider delete the information. These deletion processes should be automated in

accordance with topic-specific policies, when available and applicable. Depending on the sensitivity of information deleted, logs can track or verify that these deletion processes have happened.

To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information should be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises.

Considering that the secure deletion of some devices (e.g. smartphones) can only be achieved through destruction or using the functions embedded in these devices (e.g. "restore factory settings"), the organization should choose the appropriate method according to the classification of information handled by such devices.

Control measures described in 7.14 should be applied to physically destroy the storage device and simultaneously delete the information it contains.

An official record of information deletion is useful when analysing the cause of a possible information leakage event.

Other information

Information on user data deletion in cloud services can be found in ISO/IEC 27017.

Information on deletion of PII can be found in ISO/IEC 27555.

8.11 Data masking

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

Guidance

Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as data masking, pseudonymization or anonymization.

Pseudonymization or anonymization techniques can hide PII, disguise the true identity of PII principals or other sensitive information, and disconnect the link between PII and the identity of the PII principal or the link between other sensitive information.

When using pseudonymization or anonymization techniques, it should be verified that data has been adequately pseudonymized or anonymized. Data anonymization should consider all the elements of the sensitive information to be effective. As an example, if not considered properly, a person can be identified even if the data that can directly identify that person is anonymised, by the presence of further data which allows the person to be identified indirectly.

Additional techniques for data masking include:

- a) encryption (requiring authorized users to have a key);
- b) nulling or deleting characters (preventing unauthorized users from seeing full messages);

- c) varying numbers and dates;
- d) substitution (changing one value for another to hide sensitive data);
- e) replacing values with their hash.

The following should be considered when implementing data masking techniques:

- a) not granting all users access to all data, therefore designing queries and masks in order to show only the minimum required data to the user;
- b) there are cases where some data should not be visible to the user for some records out of a set of data; in this case, designing and implementing a mechanism for obfuscation of data (e.g. if a patient does not want hospital staff to be able to see all of their records, even in case of emergency, then the hospital staff are presented with partially obfuscated data and data can only be accessed by staff with specific roles if it contains useful information for appropriate treatment);
- c) when data are obfuscated, giving the PII principal the possibility to require that users cannot see if the data are obfuscated (obfuscation of the obfuscation; this is used in health facilities, for example if the patient does not want personnel to see that sensitive information such as pregnancies or results of blood exams has been obfuscated);
- d) any legal or regulatory requirements (e.g. requiring the masking of payment cards' information during processing or storage).

The following should be considered when using data masking, pseudonymization or anonymization:

- a) level of strength of data masking, pseudonymization or anonymization according to the usage of the processed data;
- b) access controls to the processed data;
- c) agreements or restrictions on usage of the processed data;
- d) prohibiting collating the processed data with other information in order to identify the PII principal;
- e) keeping track of providing and receiving the processed data.

Other information

Anonymization irreversibly alters PII in such a way that the PII principal can no longer be identified directly or indirectly.

Pseudonymization replaces the identifying information with an alias. Knowledge of the algorithm (sometimes referred to as the “additional information”) used to perform the pseudonymization allows for at least some form of identification of the PII principal. Such “additional information” should therefore be kept separate and protected.

While pseudonymization is therefore weaker than anonymization, pseudonymized datasets can be more useful in statistical research.

Data masking is a set of techniques to conceal, substitute or obfuscate sensitive data items. Data masking can be static (when data items are masked in the original database), dynamic (using automation and rules to secure data in real-time) or on-the-fly (with data masked in an application's memory).

Hash functions can be used in order to anonymize PII. In order to prevent enumeration attacks, they should always be combined with a salt function.

PII in resource identifiers and their attributes [e.g. file names, uniform resource locators (URLs)] should be either avoided or appropriately anonymized.

Additional controls concerning the protection of PII in public clouds are given in ISO/IEC 27018.

Additional information on de-identification techniques is available in ISO/IEC 20889.

8.12 Data leakage prevention

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence

Control

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

Guidance

The organization should consider the following to reduce the risk of data leakage:

- identifying and classifying information to protect against leakage (e.g. personal information, pricing models and product designs);
- monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);
- acting to prevent information from leaking (e.g. quarantine emails containing sensitive information).

Data leakage prevention tools should be used to:

- identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);
- detect the disclosure of sensitive information (e.g. when information is uploaded to untrusted third-party cloud services or sent via email);
- block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

The organization should determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of the organization. If that is the case, the organization should implement technology such as data leakage prevention tools or the configuration of existing tools that allow users to view and manipulate data held remotely but prevent copy and paste outside of the organization's control.

If data export is required, the data owner should be allowed to approve the export and hold users accountable for their actions.

Taking screenshots or photographs of the screen should be addressed through terms and conditions of use, training and auditing.

Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

Data leakage prevention should also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial, scientific or any other) which can be of interest for espionage or can be critical for the community. The

data leakage prevention actions should be oriented to confuse the adversary's decisions for example by replacing authentic information with false information, either as an independent action or as response to the adversary's intelligence actions. Examples of these kinds of actions are reverse social engineering or the use of honeypots to attract attackers.

Other information

Data leakage prevention tools are designed to identify data, monitor data usage and movement, and take actions to prevent data from leaking (e.g. alerting users to their risky behaviour and blocking the transfer of data to portable storage devices).

Data leakage prevention inherently involves monitoring personnel's communications and online activities, and by extension external party messages, which raises legal concerns that should be considered prior to deploying data leakage prevention tools. There is a variety of legislation relating to privacy, data protection, employment, interception of data and telecommunications that is applicable to monitoring and data processing in the context of data leakage prevention.

Data leakage prevention can be supported by standard security controls, such as topic-specific policies on access control and secure document management (see 5.12 and 5.15).

8.13 Information backup

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Control

Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

Purpose

To enable recovery from loss of data or systems.

Guidance

A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.

Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.

When designing a backup plan, the following items should be taken into consideration:

- producing accurate and complete records of the backup copies and documented restoration procedures;
- reflecting the business requirements of the organization (e.g. the recovery point objective, see 5.30), the security requirements of the information involved and the criticality of the information to the continued operation of the organization in the extent (e.g. full or differential backup) and frequency of backups;
- storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site;
- giving backup information an appropriate level of physical and environmental protection (see Clause 7 and 8.1) consistent with the standards applied at the main site;

- e) regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss;
- f) protecting backups by means of encryption according to the identified risks (e.g. in situations where confidentiality is of importance);
- g) taking care to ensure that inadvertent data loss is detected before backup is taken.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.

Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans (see 5.30). This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan. In the case of critical systems and services, backup measures should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of the organization's information, applications and systems in the cloud service environment should be taken. The organization should determine if and how requirements for backup are fulfilled when using the information backup service provided as part of the cloud service.

The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires and should take into consideration legislation and regulations.

Other information

For further information on storage security including retention consideration, see ISO/IEC 27040.

8.14 Redundancy of information processing facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Purpose

To ensure the continuous operation of information processing facilities.

Guidance

The organization should identify requirements for the availability of business services and information systems. The organization should design and implement systems architecture with appropriate redundancy to meet these requirements.

Redundancy can be introduced by duplicating information processing facilities in part or in their entirety (i.e. spare components or having two of everything). The organization should plan and implement procedures for the activation of the redundant components and processing facilities. The procedures should establish if the redundant components and processing activities are always

activated, or in case of emergency, automatically or manually activated. The redundant components and information processing facilities should ensure the same security level as the primary ones.

Mechanisms should be in place to alert the organization to any failure in the information processing facilities, enable executing the planned procedure and allow continued availability while the information processing facilities are repaired or replaced.

The organization should consider the following when implementing redundant systems:

- a) contracting with two or more suppliers of network and critical information processing facilities such as internet service providers;
- b) using redundant networks;
- c) using two geographically separate data centres with mirrored systems;
- d) using physically redundant power supplies or sources;
- e) using multiple parallel instances of software components, with automatic load balancing between them (between instances in the same data centre or in different data centres);
- f) having duplicated components in systems (e.g. CPU, hard disks, memories) or in networks (e.g. firewalls, routers, switches).

Where applicable, preferably in production mode, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

Other information

There is a strong relationship between redundancy and ICT readiness for business continuity (see 5.30) especially if short recovery times are required. Many of the redundancy measures can be part of the ICT continuity strategies and solutions.

The implementation of redundancies can introduce risks to the integrity (e.g. processes of copying data to duplicated components can introduce errors) or confidentiality (e.g. weak security control of duplicated components can lead to compromise) of information and information systems, which need to be considered when designing information systems.

Redundancy in information processing facilities does not usually address application unavailability due to faults within an application.

With the use of public cloud computing, it is possible to have multiple live versions of information processing facilities, existing in multiple separate physical locations with automatic failover and load balancing between them.

Some of the technologies and techniques for providing redundancy and automatic fail-over in the context of cloud services are discussed in ISO/IEC TS 23167.

8.15 Logging

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence

Control

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.

Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

Guidance

General

The organization should determine the purpose for which logs are created, what data is collected and logged, and any log-specific requirements for protecting and handling the log data. This should be documented in a topic-specific policy on logging.

Event logs should include for each event, as applicable:

- a) user IDs;
- b) system activities;
- c) dates, times and details of relevant events (e.g. log-on and log-off);
- d) device identity, system identifier and location;
- e) network addresses and protocols.

The following events should be considered for logging:

- a) successful and rejected system access attempts;
- b) successful and rejected data and other resource access attempts;
- c) changes to system configuration;
- d) use of privileges;
- e) use of utility programs and applications;
- f) files accessed and the type of access, including deletion of important data files;
- g) alarms raised by the access control system;
- h) activation and de-activation of security systems, such as anti-virus systems and intrusion detection systems;
- i) creation, modification or deletion of identities;
- j) transactions executed by users in applications. In some cases, the applications are a service or product provided or run by a third party.

It is important for all systems to have synchronized time sources (see 8.17) as this allows for correlation of logs between systems for analysis, alerting and investigation of an incident.

Protection of logs

Users, including those with privileged access rights, should not have permission to delete or de-activate logs of their own activities. They can potentially manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

- a) alterations to the message types that are recorded;

- b) log files being edited or deleted;
- c) failure to record events or over-writing of past recorded events if the storage media holding a log file is exceeded.

For protection of logs, the use of the following techniques should be considered: cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file.

Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence (see 5.28).

Where the organization needs to send system or application logs to a vendor to assist with debugging or troubleshooting errors, logs should be de-identified where possible using data masking techniques (see 8.11) for information such as usernames, internet protocol (IP) addresses, hostnames or organization name, before sending to the vendor.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 5.34).

Log analysis

Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behaviour, which can represent indicators of compromise.

Analysis of events should be performed by taking into account:

- a) the necessary skills for the experts performing the analysis;
- b) determining the procedure of log analysis;
- c) the required attributes of each security-related event;
- d) exceptions identified through the use of predetermined rules [e.g. security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures];
- e) known behaviour patterns and standard network traffic compared to anomalous activity and behaviour [user and entity behaviour analytics (UEBA)];
- f) results of trend or pattern analysis (e.g. as a result of using data analytics, big data techniques and specialized analysis tools);
- g) available threat intelligence.

Log analysis should be supported by specific monitoring activities to help identify and analyse anomalous behaviour, which includes:

- a) reviewing successful and unsuccessful attempts to access protected resources [e.g. domain name system (DNS) servers, web portals and file shares];
- b) checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers;
- c) examining usage reports from service providers (e.g. invoices or service reports) for unusual activity within systems and networks (e.g. by reviewing patterns of activity);
- d) including event logs of physical monitoring such as entrance and exit to ensure more accurate detection and incident analysis;
- e) correlating logs to enable efficient and highly accurate analysis.

Suspected and actual information security incidents should be identified (e.g. malware infection or probing of firewalls) and be subject to further investigation (e.g. as part of an information security incident management process, see 5.25).

Other information

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the use of suitable utility programs or audit tools to perform file interrogation can be considered.

Event logging sets the foundation for automated monitoring systems (see 8.16) which are capable of generating consolidated reports and alerts on system security.

A SIEM tool or equivalent service can be used to store, correlate, normalize and analyse log information, and to generate alerts. SIEMs tend to require careful configuration to optimize their benefits. Configurations to consider include identification and selection of appropriate log sources, tuning and testing of rules and development of use cases.

Public transparency files for the recording of logs are used, for example, in certificate transparency systems. Such files can provide an additional detection mechanism useful for guarding against log tampering.

In cloud environments, log management responsibilities can be shared between the cloud service customer and the cloud service provider. Responsibilities vary depending on the type of cloud service being used. Further guidance can be found in ISO/IEC 27017.

8.16 Monitoring activities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Purpose

To detect anomalous behaviour and potential information security incidents.

Guidance

The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.

The following should be considered for inclusion within the monitoring system:

- outbound and inbound network, system and application traffic;
- access to systems, servers, networking equipment, monitoring system, critical applications, etc.;
- critical or admin level system and network configuration files;
- logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention];
- event logs relating to system and network activity;

- f) checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code);
- g) use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance.

The organization should establish a baseline of normal behaviour and monitor against this baseline for anomalies. When establishing a baseline, the following should be considered:

- a) reviewing utilization of systems at normal and peak periods;
- b) usual time of access, location of access, frequency of access for each user or group of users.

The monitoring system should be configured against the established baseline to identify anomalous behaviour, such as:

- a) unplanned termination of processes or applications;
- b) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers);
- c) known attack characteristics (e.g. denial of service and buffer overflows);
- d) unusual system behaviour (e.g. keystroke logging, process injection and deviations in use of standard protocols);
- e) bottlenecks and overloads (e.g. network queuing, latency levels and network jitter);
- f) unauthorized access (actual or attempted) to systems or information;
- g) unauthorized scanning of business applications, systems and networks;
- h) successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems);
- i) unusual user and system behaviour in relation to expected behaviour.

Continuous monitoring via a monitoring tool should be used. Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. Monitoring tools should include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools should also be able to recognize specific signatures and data or network or application behaviour patterns.

Automated monitoring software should be configured to generate alerts (e.g. via management consoles, email messages or instant messaging systems) based on predefined thresholds. The alerting system should be tuned and trained on the organization's baseline to minimize false positives. Personnel should be dedicated to respond to alerts and should be properly trained to accurately interpret potential incidents. There should be redundant systems and processes in place to receive and respond to alert notifications.

Abnormal events should be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring (see 5.25). Procedures should be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events (see 5.26) on information security. Procedures should also be established to identify and address false positives including tuning the monitoring software to reduce the number of future false positives.

Other information

Security monitoring can be enhanced by:

- a) leveraging threat intelligence systems (see 5.7);
- b) leveraging machine learning and artificial intelligence capabilities;

Normen-Download-Beuth-Heinking Kühn Lier- Wojtek PartGmbB-KdNr. 7791402-ID.rc25i_5DuGlsklPuDu08_xSfMunqNFn210K056r-2023-07-12 11:26:52

- c) using blocklists or allowlists;
- d) undertaking a range of technical security assessments (e.g. vulnerability assessments, penetration testing, cyber-attack simulations and cyber response exercises), and using the results of these assessments to help determine baselines or acceptable behaviour;
- e) using performance monitoring systems to help establish and detect anomalous behaviour;
- f) leveraging logs in combination with monitoring systems.

Monitoring activities are often conducted using specialist software, such as intrusion detection systems. These can be configured to a baseline of normal, acceptable and expected system and network activities.

Monitoring for anomalous communications helps in the identification of botnets (i.e. set of devices under the malicious control of the botnet owner, usually used for mounting distributed denial of service attacks on other computers of other organizations). If the computer is being controlled by an external device, there is a communication between the infected device and the controller. The organization should therefore employ technologies to monitor for anomalous communications and take such action as necessary.

8.17 Clock synchronization

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Control

The clocks of information processing systems used by the organization should be synchronized to approved time sources.

Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

Guidance

External and internal requirements for time representation, reliable synchronization and accuracy should be documented and implemented. Such requirements can be from legal, statutory, regulatory, contractual, standards and internal monitoring needs. A standard reference time for use within the organization should be defined and considered for all systems, including building management systems, entry and exit systems and others that can be used to aid investigations.

A clock linked to a radio time broadcast from a national atomic clock or global positioning system (GPS) should be used as the reference clock for logging systems; a consistent, trusted date and time source to ensure accurate time-stamps. Protocols such as network time protocol (NTP) or precision time protocol (PTP) should be used to keep all networked systems in synchronization with a reference clock.

The organization can use two external time sources at the same time in order to improve the reliability of external clocks, and appropriately manage any variance.

Clock synchronization can be difficult when using multiple cloud services or when using both cloud and on-premises services. In this case, the clock of each service should be monitored and the difference recorded in order to mitigate risks arising from discrepancies.

Other information

The correct setting of computer clocks is important to ensure the accuracy of event logs, which can be required for investigations or as evidence in legal and disciplinary cases. Inaccurate audit logs can hinder such investigations and damage the credibility of such evidence.

8.18 Use of privileged utility programs

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

Control

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

Purpose

To ensure the use of utility programs does not harm system and application controls for information security.

Guidance

The following guidelines for the use of utility programs that can be capable of overriding system and application controls should be considered:

- limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 8.2);
- use of identification, authentication and authorization procedures for utility programs, including unique identification of the person who uses the utility program;
- defining and documenting of authorization levels for utility programs;
- authorization for ad hoc use of utility programs;
- not making utility programs available to users who have access to applications on systems where segregation of duties is required;
- removing or disabling all unnecessary utility programs;
- at a minimum, logical segregation of utility programs from application software. Where practical, segregating network communications for such programs from application traffic;
- limitation of the availability of utility programs (e.g. for the duration of an authorized change);
- logging of all use of utility programs.

Other information

Most information systems have one or more utility programs that can be capable of overriding system and application controls, for example diagnostics, patching, antivirus, disk defragmenters, debuggers, backup and network tools.

8.19 Installation of software on operational systems

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection

Control

Procedures and measures should be implemented to securely manage software installation on operational systems.

Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

Guidance

The following guidelines should be considered to securely manage changes and installation of software on operational systems:

- performing updates of operational software only by trained administrators upon appropriate management authorization (see 8.5);
- ensuring that only approved executable code and no development code or compilers is installed on operational systems;
- only installing and updating software after extensive and successful testing (see 8.29 and 8.31);
- updating all corresponding program source libraries;
- using a configuration control system to keep control of all operational software as well as the system documentation;
- defining a rollback strategy before changes are implemented;
- maintaining an audit log of all updates to operational software;
- archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release (e.g. the introduction of new information security functionality or the number and severity of information security vulnerabilities affecting the current version). Software patches should be applied when they can help to remove or reduce information security vulnerabilities (see 8.8 and 8.19).

Computer software can rely on externally supplied software and packages (e.g. software programs using modules which are hosted on external sites), which should be monitored and controlled to avoid unauthorized changes, because they can introduce information security vulnerabilities.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software. Open source software used in operational systems should be maintained to the latest appropriate release of the software. Over time, open source code can cease to be maintained but is still available in an open source software repository. The organization should also consider the risks of relying on unmaintained open source software when used in operational systems.

When suppliers are involved in installing or updating software, physical or logical access should only be given when necessary and with appropriate authorization. The supplier's activities should be monitored (see 5.22).

The organization should define and enforce strict rules on which types of software users can install.

The principle of least privilege should be applied to software installation on operational systems. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted based on the roles of the users concerned.

Other information

No other information.

8.20 Networks security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_net- work_security	#Protection

Control

Networks and network devices should be secured, managed and controlled to protect information in systems and applications.

Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network.

Guidance

Controls should be implemented to ensure the security of information in networks and to protect connected services from unauthorized access. In particular, the following items should be considered:

- the type and classification level of information that the network can support;
- establishing responsibilities and procedures for the management of networking equipment and devices;
- maintaining up to date documentation including network diagrams and configuration files of devices (e.g. routers, switches);
- separating operational responsibility for networks from ICT system operations where appropriate (see 5.3);
- establishing controls to safeguard the confidentiality and integrity of data passing over public networks, third-party networks or over wireless networks and to protect the connected systems and applications (see 5.22, 8.24, 5.14 and 6.6). Additional controls can also be required to maintain the availability of the network services and computers connected to the network;
- appropriately logging and monitoring to enable recording and detection of actions that can affect, or are relevant to, information security (see 8.16 and 8.15);
- closely coordinating network management activities both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

- h) authenticating systems on the network;
- i) restricting and filtering systems connection to the network (e.g. using firewalls);
- j) detecting, restricting and authenticating the connection of equipment and devices to the network;
- k) hardening of network devices;
- l) segregating network administration channels from other network traffic;
- m) temporarily isolating critical subnetworks (e.g. with drawbridges) if the network is under attack;
- n) disabling vulnerable network protocols.

The organization should ensure that appropriate security controls are applied to the use of virtualized networks. Virtualized networks also cover software-defined networking (SDN, SD-WAN). Virtualized networks can be desirable from a security viewpoint, since they can permit logical separation of communication taking place over physical networks, particularly for systems and applications that are implemented using distributed computing.

Other information

Additional information on network security can be found in the ISO/IEC 27033 series.

More information concerning virtualized networks can be found in ISO/IEC TS 23167.

8.21 Security of network services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_net- work_security	#Protection

Control

Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.

Purpose

To ensure security in the use of network services.

Guidance

The security measures necessary for particular services, such as security features, service levels and service requirements, should be identified and implemented (by internal or external network service providers). The organization should ensure that network service providers implement these measures.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored. The right to audit should be agreed between the organization and the provider. The organization should also consider third-party attestations provided by service providers to demonstrate they maintain appropriate security measures.

Rules on the use of networks and network services should be formulated and implemented to cover:

- a) the networks and network services which are allowed to be accessed;
- b) authentication requirements for accessing various network services;
- c) authorization procedures for determining who is allowed to access which networks and networked services;

- d) network management and technological controls and procedures to protect access to network connections and network services;
- e) the means used to access networks and network services [e.g. use of virtual private network (VPN) or wireless network];
- f) time, location and other attributes of the user at the time of the access;
- g) monitoring of the use of network services.

The following security features of network services should be considered:

- a) technology applied for security of network services, such as authentication, encryption and network connection controls;
- b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
- c) caching (e.g. in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements;
- d) procedures for the network service usage to restrict access to network services or applications, where necessary.

Other information

Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

More guidance on a framework for access management is given in ISO/IEC 29146.

8.22 Segregation of networks

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_net- work_security	#Protection

Control

Groups of information services, users and information systems should be segregated in the organization's networks.

Purpose

To split the network in security boundaries and to control traffic between them based on business needs.

Guidance

The organization should consider managing the security of large networks by dividing them into separate network domains and separating them from the public network (i.e. internet). The domains can be chosen based on levels of trust, criticality and sensitivity (e.g. public access domain, desktop domain, server domain, low- and high-risk systems), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks.

The perimeter of each domain should be well-defined. If access between network domains is allowed, it should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for

segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the topic-specific policy on access control (see 5.15), access requirements, value and classification of information processed and take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly-defined network perimeter. Radio coverage adjustment should be considered for segregation of wireless networks. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls (see 8.20) before granting access to internal systems. Wireless access network for guests should be segregated from those for personnel if personnel only use controlled user endpoint devices compliant to the organization's topic-specific policies. WiFi for guests should have at least the same restrictions as WiFi for personnel, in order to discourage the use of guest WiFi by personnel.

Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

8.23 Web filtering

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_net- work_security	#Protection

Control

Access to external websites should be managed to reduce exposure to malicious content.

Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

Guidance

The organization should reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material. A technique for achieving this works by blocking the IP address or domain of the website(s) concerned. Some browsers and anti-malware technologies do this automatically or can be configured to do so.

The organization should identify the types of websites to which personnel should or should not have access. The organization should consider blocking access to the following types of websites:

- websites that have an information upload function unless permitted for valid business reasons;
- known or suspected malicious websites (e.g. those distributing malware or phishing contents);
- command and control servers;
- malicious website acquired from threat intelligence (see 5.7);
- websites sharing illegal content.

Prior to deploying this control, the organization should establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. The rules should be kept up-to-date.

Training should be given to personnel on the secure and appropriate use of online resources including access to the web. The training should include the organization's rules, contact point for raising security concerns, and exception process when restricted web resources need to be accessed for legitimate business reasons. Training should also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.

Other information

Web filtering can include a range of techniques including signatures, heuristics, list of acceptable websites or domains, list of prohibited websites or domains and bespoke configuration to help prevent malicious software and other malicious activity from attacking the organization's network and systems.

8.24 Use of cryptography

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

Guidance

General

When using cryptography, the following should be considered:

- the topic-specific policy on cryptography defined by the organization, including the general principles for the protection of information. A topic-specific policy on the use of cryptography is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use;
- identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms required;
- the use of cryptography for protection of information held on mobile user endpoint devices or storage media and transmitted over networks to such devices or storage media;
- the approach to key management, including methods to deal with the generation and protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;
- roles and responsibilities for:
 - the implementation of the rules for the effective use of cryptography;

- 2) the key management, including key generation (see 8.24);
- f) the standards to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices that are approved or required for use in the organization;
- g) the impact of using encrypted information on controls that rely on content inspection (e.g. malware detection or content filtering).

When implementing the organization's rules for effective use of cryptography, the regulations and national restrictions that can apply to the use of cryptographic techniques in different parts of the world should be taken into consideration as well as the issues of trans-border flow of encrypted information (see 5.31).

The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g. with a certification authority) should cover issues of liability, reliability of services and response times for the provision of services (see 5.22).

Key management

Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

- a) generating keys for different cryptographic systems and different applications;
- b) issuing and obtaining public key certificates;
- c) distributing keys to intended entities, including how to activate keys when received;
- d) storing keys, including how authorized users obtain access to keys;
- e) changing or updating keys including rules on when to change keys and how this will be done;
- f) dealing with compromised keys;
- g) revoking keys including how to withdraw or deactivate keys [e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived)];
- h) recovering keys that are lost or corrupted;
- i) backing up or archiving keys;
- j) destroying keys;
- k) logging and auditing of key management related activities;
- l) setting activation and deactivation dates for keys so that the keys can only be used for the period of time according to the organization's rules on key management;
- m) handling legal requests for access to cryptographic keys (e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case).

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

In addition to integrity, for many use cases, the authenticity of public keys should also be considered.

Other information

The authenticity of public keys is usually addressed by public key management processes using certificate authorities and public key certificates, but it is also possible to address it by using technologies such as applying manual processes for small number keys.

Cryptography can be used to achieve different information security objectives, for example:

- a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;
- c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
- d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

The ISO/IEC 11770 series provides further information on key management.

8.25 Secure development life cycle

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net- work_security	#Protection

Control

Rules for the secure development of software and systems should be established and applied.

Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

Guidance

Secure development is a requirement to build up a secure service, architecture, software and system. To achieve this, the following aspects should be considered:

- a) separation of development, test and production environments (see 8.31);
- b) guidance on the security in the software development life cycle:
 - 1) security in the software development methodology (see 8.28 and 8.27);
 - 2) secure coding guidelines for each programming language used (see 8.28);
- c) security requirements in the specification and design phase (see 5.8);
- d) security checkpoints in projects (see 5.8);
- e) system and security testing, such as regression testing, code scan and penetration tests (see 8.29);
- f) secure repositories for source code and configuration (see 8.4 and 8.9);
- g) security in the version control (see 8.32);

- h) required application security knowledge and training (see 8.28);
- i) developers' capability for preventing, finding and fixing vulnerabilities (see 8.28);
- j) licensing requirements and alternatives to ensure cost-effective solutions while avoiding future licensing issues (See 5.32).

If development is outsourced, the organization should obtain assurance that the supplier complies with the organization's rules for secure development (see 8.30).

Other information

Development can also take place inside applications, such as office applications, scripting, browsers and databases.

8.26 Application security requirements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net-work_security	#Protection #Defence

Control

Information security requirements should be identified, specified and approved when developing or acquiring applications.

Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications.

Guidance

General

Application security requirements should be identified and specified. These requirements are usually determined through a risk assessment. The requirements should be developed with the support of information security specialists.

Application security requirements can cover a wide range of topics, depending on the purpose of the application.

Application security requirements should include, as applicable:

- a) level of trust in identity of entities [e.g. through authentication (see 5.17, 8.2 and 8.5)];
- b) identifying the type of information and classification level to be processed by the application;
- c) need for segregation of access and level of access to data and functions in the application;
- d) resilience against malicious attacks or unintentional disruptions [e.g. protection against buffer overflow or structured query language (SQL) injections];
- e) legal, statutory and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed or stored;
- f) need for privacy associated with all parties involved;
- g) the protection requirements of any confidential information;
- h) protection of data while being processed, in transit and at rest;

- i) need to securely encrypt communications between all involved parties;
- j) input controls, including integrity checks and input validation;
- k) automated controls (e.g. approval limits or dual approvals);
- l) output controls, also considering who can access outputs and its authorization;
- m) restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data (e.g. personal data);
- n) requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements;
- o) requirements mandated by other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
- p) error message handling.

Transactional services

Additionally, for applications offering transactional services between the organization and a partner, the following should be considered when identifying information security requirements:

- a) the level of trust each party requires in each other's claimed identity;
- b) the level of trust required in the integrity of information exchanged or processed and the mechanisms for identification of lack of integrity (e.g. cyclic redundancy check, hashing, digital signatures);
- c) authorization processes associated with who can approve contents of, issue or sign key transactional documents;
- d) confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation (e.g. contracts associated with tendering and contract processes);
- e) the confidentiality and integrity of any transactions (e.g. orders, delivery address details and confirmation of receipts);
- f) requirements on how long to maintain a transaction confidential;
- g) insurance and other contractual requirements.

Electronic ordering and payment applications

Additionally, for applications involving electronic ordering and payment, the following should be considered:

- a) requirements for maintaining the confidentiality and integrity of order information;
- b) the degree of verification appropriate to verify payment information supplied by a customer;
- c) avoidance of loss or duplication of transaction information;
- d) storing transaction details outside of any publicly accessible environment (e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on electronic storage media directly accessible from the internet);
- e) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate or signature management process.

Several of the above considerations can be addressed by the application of cryptography (see 8.24), taking into consideration legal requirements (see 5.31 to 5.36, especially see 5.31 for cryptography legislation).

Other information

Applications accessible via networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public; incomplete transmission, mis-routing, unauthorized message alteration, duplication or replay. Therefore, detailed risk assessments and careful determination of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Further information on application security can be found in the ISO/IEC 27034 series.

8.27 Secure system architecture and engineering principles

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net- work_security	#Protection

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.

Purpose

To ensure information systems are securely designed, implemented and operated within the development life cycle.

Guidance

Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology). New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

Secure engineering principles provide guidance on user authentication techniques, secure session control and data validation and sanitisation.

Secure system engineering principles should include analysis of:

- the full range of security controls required to protect information and systems against identified threats;
- the capabilities of security controls to prevent, detect or respond to security events;
- specific security controls required by particular business processes (e.g. encryption of sensitive information, integrity checking and digitally signing information);
- where and how security controls are to be applied (e.g. by integrating with a security architecture and the technical infrastructure);
- how individual security controls (manual and automated) work together to produce an integrated set of controls.

Security engineering principles should take account of:

- the need to integrate with a security architecture;

- b) technical security infrastructure [e.g. public key infrastructure (PKI), identity and access management (IAM), data leakage prevention and dynamic access management];
- c) capability of the organization to develop and support the chosen technology;
- d) cost, time and complexity of meeting security requirements;
- e) current good practices.

Secure system engineering should involve:

- a) the use of security architecture principles, such as “security by design”, “defence in depth”, “security by default”, “default deny”, “fail securely”, “distrust input from external applications”, “security in deployment”, “assume breach”, “least privilege”, “usability and manageability” and “least functionality”;
- b) a security-oriented design review to help identify information security vulnerabilities, ensure security controls are specified and meet security requirements;
- c) documentation and formal acknowledgement of security controls that do not fully meet requirements (e.g. due to overriding safety requirements);
- d) hardening of systems.

The organization should consider “zero trust” principles such as:

- a) assuming the organization’s information systems are already breached and thus not be reliant on network perimeter security alone;
- b) employing a “never trust and always verify” approach for access to information systems;
- c) ensuring that requests to information systems are encrypted end-to-end;
- d) verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e. not automatically trusting anything inside or outside its perimeters);
- e) using “least privilege” and dynamic access control techniques (see 5.15, 5.18 and 8.2). This includes authenticating and authorizing requests for information or to systems based on contextual information such as authentication information (see 5.17), user identities (see 5.16), data about the user endpoint device, and data classification (see 5.12);
- f) always authenticating requesters and always validating authorization requests to information systems based on information including authentication information (see 5.17) and user identities (5.16), data about the user endpoint device, and data classification (see 5.12), for example enforcing strong authentication (e.g. multi-factor, see 8.5).

The established security engineering principles should be applied, where applicable, to outsourced development of information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should ensure that suppliers’ security engineering practices align with the organization’s needs.

The security engineering principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up-to-date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

Other information

Secure engineering principles can be applied to the design or configuration of a range of techniques, such as:

- fault tolerance and other resilience techniques;
- segregation (e.g. through virtualization or containerization);
- tamper resistance.

Secure virtualization techniques can be used to prevent interference between applications running on the same physical device. If a virtual instance of an application is compromised by an attacker, only that instance is affected. The attack has no effect on any other application or data.

Tamper resistance techniques can be used to detect tampering of information containers, whether physical (e.g. a burglar alarm) or logical (e.g. a data file). A characteristic of such techniques is that there is a record of the attempt to tamper with the container. In addition, the control can prevent the successful extraction of data through its destruction (e.g. device memory can be deleted).

8.28 Secure coding

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control

Secure coding principles should be applied to software development.

Purpose

To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

Guidance

General

The organization should establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied. Additionally, such processes and governance should be extended to cover software components from third parties and open source software.

The organization should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the organization’s secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape.

Planning and before coding

Secure coding principles should be used both for new developments and in reuse scenarios. These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others. Planning and prerequisites before coding should include:

- organization-specific expectations and approved principles for secure coding to be used for both in-house and outsourced code developments;
- common and historical coding practices and defects that lead to information security vulnerabilities;

- c) configuring development tools, such as integrated development environments (IDE), to help enforce the creation of secure code;
- d) following guidance issued by the providers of development tools and execution environments as applicable;
- e) maintenance and use of updated development tools (e.g. compilers);
- f) qualification of developers in writing secure code;
- g) secure design and architecture, including threat modelling;
- h) secure coding standards and where relevant mandating their use;
- i) use of controlled environments for development.

During coding

Considerations during coding should include:

- a) secure coding practices specific to the programming languages and techniques being used;
- b) using secure programming techniques, such as pair programming, refactoring, peer review, security iterations and test-driven development;
- c) using structured programming techniques;
- d) documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;
- e) prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords, unapproved code samples and unauthenticated web services).

Testing should be conducted during and after development (see 8.29). Static application security testing (SAST) processes can identify security vulnerabilities in software.

Before software is made operational, the following should be evaluated:

- a) attack surface and the principle of least privilege;
- b) conducting an analysis of the most common programming errors and documenting that these have been mitigated.

Review and maintenance

After code has been made operational:

- a) updates should be securely packaged and deployed;
- b) reported information security vulnerabilities should be handled (see 8.8);
- c) errors and suspected attacks should be logged and logs regularly reviewed to make adjustments to the code as necessary;
- d) source code should be protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control).

If using external tools and libraries, the organization should consider:

- a) ensuring that external libraries are managed (e.g. by maintaining an inventory of libraries used and their versions) and regularly updated with release cycles;

- b) selection, authorization and reuse of well-vetted components, particularly authentication and cryptographic components;
- c) the licence, security and history of external components;
- d) ensuring that software is maintainable, tracked and originates from proven, reputable sources;
- e) sufficiently long-term availability of development resources and artefacts.

Where a software package needs to be modified the following points should be considered:

- a) the risk of built-in controls and integrity processes being compromised;
- b) whether to obtain the consent of the vendor;
- c) the possibility of obtaining the required changes from the vendor as standard program updates;
- d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes;
- e) compatibility with other software in use.

Other information

A guiding principle is to ensure security-relevant code is invoked when necessary and is tamper-resistant. Programs installed from compiled binary code also have these properties but only for data held within the application. For interpreted languages, the concept only works when the code is executed on a server that is otherwise inaccessible by the users and processes that use it, and that its data is held in a similarly protected database. For example, the interpreted code can be run on a cloud service where access to the code itself requires administrator privileges. Such administrator access should be protected by security mechanisms such as just-in-time administration principles and strong authentication. If the application owner can access scripts by direct remote access to the server, so in principle can an attacker. Web servers should be configured to prevent directory browsing in such cases.

Application code is best designed on the assumption that it is always subject to attack, through error or malicious action. In addition, critical applications can be designed to be tolerant of internal faults. For example, the output from a complex algorithm can be checked to ensure that it lies within safe bounds before the data is used in an application such as a safety or financial critical application. The code that performs the boundary checks is simple and therefore much easier to prove correctness.

Some web applications are susceptible to a variety of vulnerabilities that are introduced by poor design and coding, such as database injection and cross-site scripting attacks. In these attacks, requests can be manipulated to abuse the webserver functionality.

More information on ICT security evaluation can be found in the ISO/IEC 15408 series.

8.29 Security testing in development and acceptance

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection

Control

Security testing processes should be defined and implemented in the development life cycle.

Purpose

To validate if information security requirements are met when applications or code are deployed to the production environment.

Guidance

New information systems, upgrades and new versions should be thoroughly tested and verified during the development processes. Security testing should be an integral part of the testing for systems or components.

Security testing should be conducted against a set of requirements, which can be expressed as functional or non-functional. Security testing should include testing of:

- a) security functions [e.g. user authentication (see 8.5), access restriction (see 8.3) and use of cryptography (see 8.24)];
- b) secure coding (see 8.28);
- c) secure configurations (see 8.9, 8.20 and 8.22) including that of operating systems, firewalls and other security components.

Test plans should be determined using a set of criteria. The extent of testing should be in proportion to the importance, nature of the system and the potential impact of the change being introduced. The test plan should include:

- a) detailed schedule of activities and tests;
- b) inputs and expected outputs under a range of conditions;
- c) criteria to evaluate the results;
- d) decision for further actions as necessary.

The organization can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken to ensure that the system works as expected and only as expected (see 5.8). The following should be considered:

- a) performing code review activities as a relevant element for testing for security flaws, including un-anticipated inputs and conditions;
- b) performing vulnerability scanning to identify insecure configurations and system vulnerabilities;
- c) performing penetration testing to identify insecure code and design.

For outsourced development and purchasing components, an acquisition process should be followed. Contracts with the supplier should address the identified security requirements (see 5.20). Products and services should be evaluated against these criteria before acquisition.

Testing should be performed in a test environment that matches the target production environment as closely as possible to ensure that the system does not introduce vulnerabilities to the organization's environment and that the tests are reliable (see 8.31).

Other information

Multiple test environments can be established, which can be used for different kinds of testing (e.g. functional and performance testing). These different environments can be virtual, with individual configurations to simulate a variety of operating environments.

Testing and monitoring of test environments, tools and technologies also needs to be considered to ensure effective testing. The same considerations apply to monitoring of the monitoring systems deployed in development, test and production settings. Judgement is needed, guided by the sensitivity of the systems and data, to determine how many layers of meta-testing are useful.

8.30 Outsourced development

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_ security #Application_security #Supplier_relationships_ security	#Governance_and_ Ecosystem #Protection

Control

The organization should direct, monitor and review the activities related to outsourced system development.

Purpose

To ensure information security measures required by the organization are implemented in outsourced system development.

Guidance

Where system development is outsourced, the organization should communicate and agree requirements and expectations, and continually monitor and review whether the delivery of outsourced work meets these expectations. The following points should be considered across the organization's entire external supply chain:

- licensing agreements, code ownership and intellectual property rights related to the outsourced content (see 5.32);
- contractual requirements for secure design, coding and testing practices (see 8.25 to 8.29);
- provision of the threat model to consider by external developers;
- acceptance testing for the quality and accuracy of the deliverables (see 8.29);
- provision of evidence that minimum acceptable levels of security and privacy capabilities are established (e.g. assurance reports);
- provision of evidence that sufficient testing has been applied to guard against the presence of malicious content (both intentional and unintentional) upon delivery;
- provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;
- escrow agreements for the software source code (e.g. if the supplier goes out of business);
- contractual right to audit development processes and controls;
- security requirements for the development environment (see 8.31);
- taking consideration of applicable legislation (e.g. on protection of personal data).

Other information

Further information on supplier relationships can be found in the ISO/IEC 27036 series.

8.31 Separation of development, test and production environments

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net-work_security	#Protection

Control

Development, testing and production environments should be separated and secured.

Purpose

To protect the production environment and data from compromise by development and test activities.

Guidance

The level of separation between production, testing and development environments that is necessary to prevent production problems should be identified and implemented.

The following items should be considered:

- adequately separating development and production systems and operating them in different domains (e.g. in separate virtual or physical environments);
- defining, documenting and implementing rules and authorization for the deployment of software from development to production status;
- testing changes to production systems and applications in a testing or staging environment prior to being applied to production systems (see 8.29);
- not testing in production environments except in circumstances that have been defined and approved;
- compilers, editors and other development tools or utility programs not being accessible from production systems when not required;
- displaying appropriate environment identification labels in menus to reduce the risk of error;
- not copying sensitive information into the development and testing system environments unless equivalent controls are provided for the development and testing systems.

In all cases, development and testing environments should be protected considering:

- patching and updating of all the development, integration and testing tools (including builders, integrators, compilers, configuration systems and libraries);
- secure configuration of systems and software;
- control of access to the environments;
- monitoring of change to the environment and code stored therein;
- secure monitoring of the environments;
- taking backups of the environments.

A single person should not have the ability to make changes to both development and production without prior review and approval. This can be achieved for example through segregation of access rights or through rules that are monitored. In exceptional situations, additional measures such as detailed logging and real-time monitoring should be implemented in order to detect and act on unauthorized changes.

Normen-Download-Beuth-Heinking Kühn Lier-Wojtek PartGmbH-KdNr. 7791402-ID.rc251_5DuGlsklPuDu08_xSfMunqvNFN210K056r-2023-07-12 11:26:52

Other information

Without adequate measures and procedures, developers and testers having access to production systems can introduce significant risks (e.g. unwanted modification of files or system environment, system failure, running unauthorized and untested code in production systems, disclosure of confidential data, data integrity and availability issues). There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the production environment.

Measures and procedures include carefully designed roles in conjunction with implementing segregation of duty requirements and having adequate monitoring processes in place.

Development and testing personnel also pose a threat to the confidentiality of production information. Development and testing activities can cause unintended changes to software or information if they share the same computing environment. Separating development, testing and production environments is therefore desirable to reduce the risk of accidental change or unauthorized access to production software and business data (see 8.33 for the protection of test information).

In some cases, the distinction between development, test and production environments can be deliberately blurred and testing can be carried out in a development environment or through controlled rollouts to live users or servers (e.g. small population of pilot users). In some cases, product testing can occur through live use of the product inside the organization. Furthermore, to reduce downtime of live deployments, two identical production environments can be supported where only one is live at any one time.

Supporting processes for the use of production data in development and testing environments (8.33) are necessary.

Organizations can also consider the guidance provided in this section for training environments when conducting end user training.

8.32 Change management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net-work_security	#Protection

Control

Changes to information processing facilities and information systems should be subject to change management procedures.

Purpose

To preserve information security when executing changes.

Guidance

Introduction of new systems and major changes to existing systems should follow agreed rules and a formal process of documentation, specification, testing, quality control and managed implementation. Management responsibilities and procedures should be in place to ensure satisfactory control of all changes.

Change control procedures should be documented and enforced to ensure the confidentiality, integrity and availability of information in information processing facilities and information systems, for the entire system development life cycle from the early design stages through all subsequent maintenance efforts.

Wherever practicable, change control procedures for ICT infrastructure and software should be integrated.

The change control procedures should include:

- a) planning and assessing the potential impact of changes considering all dependencies;
- b) authorization of changes;
- c) communicating changes to relevant interested parties;
- d) tests and acceptance of tests for the changes (see 8.29);
- e) implementation of changes including deployment plans;
- f) emergency and contingency considerations including fall-back procedures;
- g) maintaining records of changes that include all of the above;
- h) ensuring that operating documentation (see 5.37) and user procedures are changed as necessary to remain appropriate;
- i) ensuring that ICT continuity plans and response and recovery procedures (see 5.30) are changed as necessary to remain appropriate.

Other information

Inadequate control of changes to information processing facilities and information systems is a common cause of system or security failures. Changes to the production environment, especially when transferring software from development to operational environment, can impact on the integrity and availability of applications.

Changing software can impact the production environment and vice versa.

Good practice includes the testing of ICT components in an environment segregated from both the production and development environments (see 8.31). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Production environment includes operating systems, databases and middleware platforms. The control should be applied for changes of applications and infrastructures.

8.33 Test information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

Control

Test information should be appropriately selected, protected and managed.

Purpose

To ensure relevance of testing and protection of operational information used for testing.

Guidance

Test information should be selected to ensure the reliability of tests results and the confidentiality of the relevant operational information. Sensitive information (including personally identifiable information) should not be copied into the development and testing environments (see 8.31).

The following guidelines should be applied to protect the copies of operational information, when used for testing purposes, whether the test environment is built in-house or on a cloud service:

- a) applying the same access control procedures to test environments as those applied to operational environments;
- b) having a separate authorization each time operational information is copied to a test environment;
- c) logging the copying and use of operational information to provide an audit trail;
- d) protecting sensitive information by removal or masking (see 8.11) if used for testing;
- e) properly deleting (see 8.10) operational information from a test environment immediately after the testing is complete to prevent unauthorized use of test information.

Test information should be securely stored (to prevent tampering, which can otherwise lead to invalid results) and only used for testing purposes.

Other information

System and acceptance testing can require substantial volumes of test information that are as close as possible to operational information.

8.34 Protection of information systems during audit testing

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

Control

Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.

Purpose

To minimize the impact of audit and other assurance activities on operational systems and business processes.

Guidance

The following guidelines should be observed:

- a) agreeing audit requests for access to systems and data with appropriate management;
- b) agreeing and controlling the scope of technical audit tests;
- c) limiting audit tests to read-only access to software and data. If read-only access is not available to obtain the necessary information, executing the test by an experienced administrator who has the necessary access rights on behalf of the auditor;
- d) if access is granted, establishing and verifying the security requirements (e.g. antivirus and patching) of the devices used for accessing the systems (e.g. laptops or tablets) before allowing the access;
- e) only allowing access other than read-only for isolated copies of system files, deleting them when the audit is completed, or giving them appropriate protection if there is an obligation to keep such files under audit documentation requirements;

- f) identifying and agreeing on requests for special or additional processing, such as running audit tools;
- g) running audit tests that can affect system availability outside business hours;
- h) monitoring and logging all access for audit and test purposes.

Other information

Audit tests and other assurance activities can also happen on development and test systems, where such tests can impact for example the integrity of code or lead to disclosure of any sensitive information held in such environments.

Annex A (informative)

Using attributes

A.1 General

This annex provides a table to demonstrate the use of attributes as a way of creating different views of the controls. The five examples of attributes are (see 4.2):

- a) Control types (#Preventive, #Detective, #Corrective)
- b) Information security properties (#Confidentiality, #Integrity, #Availability)
- c) Cybersecurity concepts (#Identify, #Protect, #Detect, #Respond, #Recover)
- d) Operational capabilities (#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance)
- e) Security domains (#Governance_and_Ecosystem, #Protection, #Defence, #Resilience)

Table A.1 contains a matrix of all controls in this document with their given attribute values.

The filtering or sorting of the matrix can be achieved by using a tool such as a simple spreadsheet or a database, which can include more information like control text, guidance, organization-specific guidance or attributes (see A.2).

Table A.1 — Matrix of controls and attribute values

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecu- ty concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosys- tem #Resil- ience
5.2	Information security roles and responsi- bilities	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Governance	#Govern- ance_and_ Ecosystem #Protection #Resilience
5.3	Segregation of duties	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Governance #Identity_and_ access_man- agement	#Governance_ and_Ecosys- tem
5.4	Management responsibili- ties	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Governance	#Governance_ and_Ecosys- tem

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Re- silience
5.6	Contact with special inter- est groups	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Threat intelli- gence	#Preventive #Detective #Corrective	#Confidential- ity #Integrity #Availability	#Identify #De- tect #Respond	#Threat_and_ vulnerability_ management	#Defence #Re- silience
5.8	Information security in project man- agement	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Governance	#Governance_ and_Ecosys- tem #Protec- tion
5.9	Inventory of information and other associated assets	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Asset_man- agement	#Governance_ and_Ecosys- tem #Protec- tion
5.10	Acceptable use of information and other associated assets	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement #Information_ protection	#Governance_ and_Ecosys- tem #Protec- tion
5.11	Return of assets	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement	#Protection
5.12	Classification of information	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Information_ protection	#Protection #Defence
5.13	Labelling of information	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection
5.14	Information transfer	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement #Information_ protection	#Protection
5.15	Access control	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection
5.16	Identity man- agement	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection
5.17	Authentication information	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection
5.18	Access rights	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
5.19	Information security in supplier relationships	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_re- lationships_se- curity	#Governance_ and_Ecosys- tem #Protec- tion
5.20	Addressing information security with-in supplier agreements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_re- lationships_se- curity	#Governance_ and_Ecosys- tem #Protec- tion
5.21	Managing information security in the ICT supply chain	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_re- lationships_se- curity	#Governance_ and_Ecosys- tem #Protec- tion
5.22	Monitor- ing, review and change management of supplier services	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_re- lationships_se- curity #Informa- tion_secu- rity_assurance	#Governance_ and_Ecosys- tem #Protec- tion #Defence
5.23	Information security for use of cloud services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_re- lationships_se- curity	#Governance_ and_Ecosys- tem #Protec- tion
5.24	Information security inci- dent manage- ment planning and prepara- tion	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Informa- tion_secu- rity_event_man- agement	#Defence
5.25	Assessment and decision on informa- tion security events	#Detective	#Confidentiality #Integrity #Availability	#Detect #Re- spond	#Informa- tion_secu- rity_event_man- agement	#Defence
5.26	Response to information security inci- dents	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Informa- tion_secu- rity_event_man- agement	#Defence
5.27	Learning from information security inci- dents	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Informa- tion_secu- rity_event_man- agement	#Defence
5.28	Collection of evidence	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Re- spond	#Informa- tion_secu- rity_event_man- agement	#Defence
5.29	Information security dur- ing disruption	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Re- spond	#Continuity	#Protection #Resilience
5.30	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
5.31	Legal, statuto- ry, regulatory and contrac- tual require- ments	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosys- tem #Protec- tion
5.32	Intellectual property rights	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Legal_and_ compliance	#Governance_ and_Ecosys- tem
5.33	Protection of records	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Asset_man- agement #Information_ protection	#Defence
5.34	Privacy and protection of PII	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Information_ protection #Legal_and_ compliance	#Protection
5.35	Independent review of information security	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Information_ security_as- surance	#Governance_ and_Ecosys- tem
5.36	Compliance with policies, rules and standards for information security	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Legal_and_ compliance #Information_ security_as- surance	#Governance_ and_Ecosys- tem
5.37	Documented operating procedures	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Protect #Re- cover	#Asset_man- agement #Physi- cal_security #System_and_ network_secu- rity #Applica- tion_security #Secure_con- figuration #Identity_ and_access_ management #Threat_and_ vulnerability_ management #Continuity #Informa- tion_securi- ty_event_man- agement	#Governance_ and_Ecosys- tem #Protec- tion #Defence
6.1	Screening	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Human_re- source_secu- rity	#Governance_ and_Ecosys- tem

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
6.2	Terms and conditions of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.3	Information security awareness, education and training	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.4	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem
6.5	Responsibilities after termination or change of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem
6.6	Confidentiality or non-disclosure agreements	#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem
6.7	Remote working	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection
6.8	Information security event reporting	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence
7.1	Physical security perimeters	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
7.2	Physical entry	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection
7.3	Securing offices, rooms and facilities	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
7.4	Physical security monitoring	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
7.5	Protect- ing against physical and environmental threats	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity	#Protection
7.6	Working in secure areas	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity	#Protection
7.7	Clear desk and clear screen	#Preventive	#Confidenti- ality	#Protect	#Physical_se- curity	#Protection
7.8	Equipment siting and protection	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity #Asset_ management	#Protection
7.9	Security of as- sets off-prem- ises	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity #Asset_ management	#Protection
7.10	Storage media	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity #Asset_ management	#Protection
7.11	Supporting utilities	#Preventive #Detective	#Integrity #Availability	#Protect #De- tect	#Physical_se- curity	#Protection
7.12	Cabling secu- rity	#Preventive	#Confidenti- ality #Availa- bility	#Protect	#Physical_se- curity	#Protection
7.13	Equipment maintenance	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Physical_se- curity #Asset_ management	#Protection #Resilience
7.14	Secure dispos- al or re-use of equipment	#Preventive	#Confidenti- ality	#Protect	#Physical_se- curity #Asset_ management	#Protection
8.1	User endpoint devices	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement #Information_ protection	#Protection
8.2	Privileged access rights	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection
8.3	Information access restric- tion	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection
8.4	Access to source code	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_ and_access_ management #Applica- tion_security #Secure_con- figuration	#Protection
8.5	Secure authen- tication	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Identity_and_ access_man- agement	#Protection

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
8.6	Capacity man- agement	#Preventive #Detective	#Integrity #Availability	#Identify #Protect #De- tect	#Continuity	#Governance_ and_Ecosys- tem #Protec- tion
8.7	Protection against mal- ware	#Preventive #Detective #Corrective	#Confidential- ity #Integrity #Availability	#Protect #De- tect	#System_and_ network_secu- rity #Informa- tion_protec- tion	#Protection #Defence
8.8	Management of technical vulnerabilities	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosys- tem #Protec- tion #Defence
8.9	Configuration management	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Secure_con- figuration	#Protection
8.10	Information deletion	#Preventive	#Confidenti- ality	#Protect	#Information_ protection #Legal_and_ compliance	#Protection
8.11	Data masking	#Preventive	#Confidenti- ality	#Protect	#Information_ protection	#Protection
8.12	Data leakage prevention	#Preventive #Detective	#Confidenti- ality	#Protect #De- tect	#Information_ protection	#Protection #Defence
8.13	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.14	Redundancy of information processing facilities	#Preventive	#Availability	#Protect	#Continuity #Asset_man- agement	#Protection #Resilience
8.15	Logging	#Detective	#Confidential- ity #Integrity #Availability	#Detect	#Informa- tion_securi- ty_event_man- agement	#Protection #Defence
8.16	Monitoring activities	#Detective #Corrective	#Confidential- ity #Integrity #Availability	#Detect #Re- spond	#Informa- tion_securi- ty_event_man- agement	#Defence
8.17	Clock synchro- nization	#Detective	#Integrity	#Protect #De- tect	#Informa- tion_securi- ty_event_man- agement	#Protection #Defence
8.18	Use of privi- leged utility programs	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#System_and_ network_secu- rity #Secure_ configuration #Application_ security	#Protection
8.19	Installation of software on operational systems	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Secure_con- figuration #Application_ security	#Protection

Table A.1 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.20	Networks security	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection
8.21	Security of network services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.22	Segregation of networks	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.23	Web filtering	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.24	Use of cryptography	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
8.25	Secure development life cycle	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.26	Application security requirements	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence
8.27	Secure system architecture and engineering principles	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.28	Secure coding	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.29	Security testing in development and acceptance	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection
8.30	Outsourced development	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Table A.1 (continued)

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.31	Separation of development, test and production environments	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.32	Change management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.33	Test information	#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection
8.34	Protection of information systems during audit testing	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

Table A.2 shows an example of how to create a view by filtering by a particular attribute value, in this case #Corrective.

Table A.2 — View of #Corrective controls

ISO/IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
5.24	Information security incident management planning and preparation	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.26	Response to information security incidents	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
5.28	Collection of evidence	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Table A.2 (continued)

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecuri- ty concepts	Operational capabilities	Security domains
5.29	Information security during disruption	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.35	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_as- surance	#Governance_and_Ecosys- tem
5.37	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_secu- rity #Application_security #Secure_configuration #Identity_and_access_ management #Threat_and_vulnerability_ management #Continuity #Information_security_event_man- agement	#Governance_and_Ecosys- tem #Protection #Defence
6.4	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_secu- rity	#Governance_and_Ecosys- tem
8.7	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_secu- rity #Information_protec- tion	#Protection #Defence
8.13	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.16	Monitoring activities	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_man- agement	#Defence

A.2 Organizational views

Since attributes are used to create different views of controls, organizations can discard the examples of attributes proposed in this document and create their own attributes with different values to address specific needs in the organization. In addition, the values assigned to each attribute can differ between organizations since organizations can have different views on the use or applicability of the control or of the values associated to the attribute (when the values are specific to the context of the

organization). The first step is to understand why an organizational-specific attribute is desirable. For example, if an organization has constructed its risk treatment plans [see ISO/IEC 27001:2013, 6.1.3 e)] based on events, it can wish to associate a risk scenario attribute to each control in this document.

The benefit of such an attribute is to speed up the process of fulfilment of ISO/IEC 27001 requirement related to risk treatment, which is to compare the controls determined through the process of risk treatment (referred to as “necessary” controls), with those in ISO/IEC 27001:2013, Annex A (which are issued from in this document) to ensure that no necessary control has been overlooked.

Once the purpose and benefits are known, the next step is to determine the attribute values. For example, the organization might identify 9 events:

- 1) loss or theft of mobile device;
- 2) loss or theft from organization's premises;
- 3) force majeure, vandalism and terrorism;
- 4) failure of software, hardware, power, internet and communications;
- 5) fraud;
- 6) hacking;
- 7) disclosure;
- 8) breach of the law;
- 9) social engineering.

The second step can therefore be accomplished by assigning identifiers to each event (e.g. E1, E2, ..., E9).

The third step is to copy the control identifiers and control names from this document into a spreadsheet or database and associate the attribute values with each control, remembering that each control can have more than one attribute value.

The final step is to sort the spreadsheet or query the database to extract the required information.

Other examples of organizational attributes (and possible values) include:

- a) maturity (values from the ISO/IEC 33000 series or other maturity models);
- b) implementation state (to do, in progress, partially implemented, fully implemented);
- c) priority (1, 2, 3, etc.);
- d) organizational areas involved (security, ICT, human resources, top management, etc.);
- e) events;
- f) assets involved;
- e) build and run, to differentiate controls used in the different steps of the service life cycle;
- g) other frameworks the organization works with or can be transitioning from.

Annex B (informative)

Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27002:2013 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27002:2013.

**Table B.1 — Correspondence between controls in this document and controls in
ISO/IEC 27002:2013**

ISO/ IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events

Table B.1 (continued)

ISO/ IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.26	16.1.5	Response to information security incidents
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	07.1.1	Screening
6.2	07.1.2	Terms and conditions of employment
6.3	07.2.2	Information security awareness, education and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	06.2.1, 11.2.8	User endpoint devices
8.2	09.2.3	Privileged access rights
8.3	09.4.1	Information access restriction
8.4	09.4.5	Access to source code
8.5	09.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware

Table B.1 (continued)

ISO/ IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	09.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development life cycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.33	14.3.1	Test information
8.34	12.7.1	Protection of information systems during audit testing

Table B.2 provides the correspondence of controls specified in ISO/IEC 27002:2013 with those in this document.

Table B.2 — Correspondence between controls in ISO/IEC 27002:2013 and controls in this document

ISO/IEC 27002:2013 control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security
5.1.2	5.1	Review of the policies for information security
6		Organization of information security

Table B.2 (continued)

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
6.1		Internal organization
6.1.1	5.2	Information security roles and responsibilities
6.1.2	5.3	Segregation of duties
6.1.3	5.5	Contact with authorities
6.1.4	5.6	Contact with special interest groups
6.1.5	5.8	Information security in project management
6.2		Mobile devices and teleworking
6.2.1	8.1	Mobile device policy
6.2.2	6.7	Teleworking
7		Human resource security
7.1		Prior to employment
7.1.1	6.1	Screening
7.1.2	6.2	Terms and conditions of employment
7.2		During employment
7.2.1	5.4	Management responsibilities
7.2.2	6.3	Information security awareness, education and training
7.2.3	6.4	Disciplinary process
7.3		Termination and change of employment
7.3.1	6.5	Termination or change of employment responsibilities
8		Asset management
8.1		Responsibility for assets
8.1.1	5.9	Inventory of assets
8.1.2	5.9	Ownership of assets
8.1.3	5.10	Acceptable use of assets
8.1.4	5.11	Return of assets
8.2		Information classification
8.2.1	5.12	Classification of information
8.2.2	5.13	Labelling of information
8.2.3	5.10	Handling of assets
8.3		Media handling
8.3.1	7.10	Management of removable media
8.3.2	7.10	Disposal of media
8.3.3	7.10	Physical media transfer
9		Access control
9.1		Business requirements of access control
9.1.1	5.15	Access control policy
9.1.2	5.15	Access to networks and network services
9.2		User access management
9.2.1	5.16	User registration and de-registration
9.2.2	5.18	User access provisioning
9.2.3	8.2	Management of privileged access rights
9.2.4	5.17	Management of secret authentication information of users

Table B.2 (continued)

ISO/IEC 27002:2013 control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
9.2.5	5.18	Review of user access rights
9.2.6	5.18	Removal or adjustment of access rights
9.3		User responsibilities
9.3.1	5.17	Use of secret authentication information
9.4		System and application access control
9.4.1	8.3	Information access restriction
9.4.2	8.5	Secure log-on procedures
9.4.3	5.17	Password management system
9.4.4	8.18	Use of privileged utility programs
9.4.5	8.4	Access control to program source code
10		Cryptography
10.1		Cryptographic controls
10.1.1	8.24	Policy on the use of cryptographic controls
10.1.2	8.24	Key management
11		Physical and environmental security
11.1		Secure areas
11.1.1	7.1	Physical security perimeter
11.1.2	7.2	Physical entry controls
11.1.3	7.3	Securing offices, rooms and facilities
11.1.4	7.5	Protecting against external and environmental threats
11.1.5	7.6	Working in secure areas
11.1.6	7.2	Delivery and loading areas
11.2		Equipment
11.2.1	7.8	Equipment siting and protection
11.2.2	7.11	Supporting utilities
11.2.3	7.12	Cabling security
11.2.4	7.13	Equipment maintenance
11.2.5	7.10	Removal of assets
11.2.6	7.9	Security of equipment and assets off-premises
11.2.7	7.14	Secure disposal or reuse of equipment
11.2.8	8.1	Unattended user equipment
11.2.9	7.7	Clear desk and clear screen policy
12		Operations security
12.1		Operational procedures and responsibilities
12.1.1	5.37	Documented operating procedures
12.1.2	8.32	Change management
12.1.3	8.6	Capacity management
12.1.4	8.31	Separation of development, testing and operational environments
12.2		Protection from malware
12.2.1	8.7	Controls against malware
12.3		Backup
12.3.1	8.13	Information backup

Table B.2 (continued)

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
12.4		Logging and monitoring
12.4.1	8.15	Event logging
12.4.2	8.15	Protection of log information
12.4.3	8.15	Administrator and operator logs
12.4.4	8.17	Clock synchronization
12.5		Control of operational software
12.5.1	8.19	Installation of software on operational systems
12.6		Technical vulnerability management
12.6.1	8.8	Management of technical vulnerabilities
12.6.2	8.19	Restrictions on software installation
12.7		Information systems audit considerations
12.7.1	8.34	Information systems audit controls
13		Communications security
13.1		Network security management facilities.
13.1.1	8.20	Network controls
13.1.2	8.21	Security of network services
13.1.3	8.22	Segregation in networks
13.2		Information transfer
13.2.1	5.14	Information transfer policies and procedures
13.2.2	5.14	Agreements on information transfer
13.2.3	5.14	Electronic messaging
13.2.4	6.6	Confidentiality or nondisclosure agreements
14		System acquisition, development and maintenance
14.1		Security requirements of information systems
14.1.1	5.8	Information security requirements analysis and specification
14.1.2	8.26	Securing application services on public networks
14.1.3	8.26	Protecting application services transactions
14.2		Security in development and support processes
14.2.1	8.25	Secure development policy
14.2.2	8.32	System change control procedures
14.2.3	8.32	Technical review of applications after operating platform changes
14.2.4	8.32	Restrictions on changes to software packages
14.2.5	8.27	Secure system engineering principles
14.2.6	8.31	Secure development environment
14.2.7	8.30	Outsourced development
14.2.8	8.29	System security testing
14.2.9	8.29	System acceptance testing
14.3		Test data
14.3.1	8.33	Protection of test data
15		Supplier relationships
15.1		Information security in supplier relationships
15.1.1	5.19	Information security policy for supplier relationships

Table B.2 (continued)

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
15.1.2	5.20	Addressing security within supplier agreements
15.1.3	5.21	Information and communication technology supply chain
15.2		Supplier service delivery management
15.2.1	5.22	Monitoring and review of supplier services
15.2.2	5.22	Managing changes to supplier services
16		Information security incident management
16.1		Management of information security incidents and improvements
16.1.1	5.24	Responsibilities and procedures
16.1.2	6.8	Reporting information security events
16.1.3	6.8	Reporting information security weaknesses
16.1.4	5.25	Assessment of and decision on information security events
16.1.5	5.26	Response to information security incidents
16.1.6	5.27	Learning from information security incidents
16.1.7	5.28	Collection of evidence
17		Information security aspects of business continuity management
17.1		Information security continuity
17.1.1	5.29	Planning information security continuity
17.1.2	5.29	Implementing information security continuity
17.1.3	5.29	Verify, review and evaluate information security continuity
17.2		Redundancies
17.2.1	8.14	Availability of information processing facilities
18		Compliance
18.1		Compliance with legal and contractual requirements
18.1.1	5.31	Identification of applicable legislation and contractual requirements
18.1.2	5.32	Intellectual property rights
18.1.3	5.33	Protection of records
18.1.4	5.34	Privacy and protection of personally identifiable information
18.1.5	5.31	Regulation of cryptographic controls
18.2		Information security reviews
18.2.1	5.35	Independent review of information security
18.2.2	5.36	Compliance with security policies and standards
18.2.3	5.36, 8.8	Technical compliance review

Bibliography

- [1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
- [2] ISO 55001, *Asset management — Management systems — Requirements*
- [3] ISO/IEC 11770 (all parts), *Information security — Key management*
- [4] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*
- [5] ISO 15489 (all parts), *Information and documentation — Records management*
- [6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
- [7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
- [8] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*
- [9] ISO/IEC 19770 (all parts), *Information technology — IT asset management*
- [10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- [11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
- [12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
- [13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
- [14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
- [15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
- [16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
- [17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
- [18] ISO/IEC TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
- [19] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
- [20] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*
- [21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
- [22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
- [23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
- [24] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

- [25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*
- [26] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
- [27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- [28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- [29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
- [30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
- [31] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*
- [32] ISO/IEC 27034 (all parts), *Information technology — Application security*
- [33] ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information security incident management*
- [34] ISO/IEC 27036 (all parts), *Information technology — Security techniques — Information security for supplier relationships*
- [35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
- [36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
- [37] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*
- [38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
- [39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
- [40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
- [41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
- [42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
- [43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*
- [44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
- [45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
- [46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
- [47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
- [48] ISO 31000:2018, *Risk management — Guidelines*
- [49] IEC 31010, *Risk management — Risk assessment techniques*

- [50] ISO/IEC 22123 (all parts), *Information technology — Cloud computing*
- [51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*
- [52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at <https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/>
- [53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076
- [54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-37r2>
- [55] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
- [56] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at <https://github.com/OWASP/DevGuide>
- [57] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at <https://doi.org/10.6028/NIST.SP.800-63b>
- [58] OASIS, Structured Threat Information Expression. Available at <https://www.oasis-open.org/standards#stix2.0>
- [59] OASIS, Trusted Automated Exchange of Indicator Information. Available at <https://www.oasis-open.org/standards#taxii2.0>