DIN EN ISO/IEC 27002

ICS 35.030

Ersatz für
DIN EN ISO/IEC 27002:2017-06

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

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

Gesamtumfang 209 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

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 EN ISO/IEC 27002:2022 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).

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

ISO 9000	siehe	DIN EN ISO 9000
ISO 21500	siehe	DIN ISO 21500
ISO 22301	siehe	DIN EN ISO 22301
ISO 22313	siehe	DIN EN ISO 22313
ISO 27799	siehe	DIN EN ISO 27799
ISO 55001	siehe	DIN ISO 55001
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 24760 (alle Teile)		DIN EN ISO/IEC 24760 (alle Teile)
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27007	siehe	DIN EN ISO/IEC 27007
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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 des Dokumentes.

Frühere Ausgaben

DIN ISO/IEC 27002: 2008-09, 2016-11
DIN EN ISO/IEC 27002: 2017-06

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

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 24760 (alle Teile), *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement*

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 27007, *Informationssicherheit, Cybersicherheit und Datenschutz — Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen*

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*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

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 21500, *Leitlinien Projektmanagement**

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*

---

* DIN ISO 21500:2016-02, *Leitlinien Projektmanagement (ISO 21500:2012)* ist zurzeit in Überarbeitung; aktueller Stand: E DIN ISO 21500:2021-12, *Projekt-, Programm- und Portfoliomanagement — Kontext und Konzepte (ISO 21500:2021); Text Deutsch und Englisch*

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

— Leerseite —

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27002

November 2022

ICS 35.030

Ersetzt EN ISO/IEC 27002:2017

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection — Information security controls (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)

Diese Europäische Norm wurde vom CEN am 30. Oktober 2022 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

Inhalt

Seite

Europäisches Vorwort ... 5
Vorwort ... 6
Einleitung ... 7
1 Anwendungsbereich ... 10
2 Normative Verweisungen ... 10
3 Begriffe und Abkürzungen ... 10
3.1 Begriffe ... 10
3.2 Abkürzungen ... 16
4 Aufbau dieses Dokuments ... 17
4.1 Abschnitte ... 17
4.2 Themen und Attribute ... 18
4.3 Maßnahmengestaltung ... 19
5 Organisatorische Maßnahmen ... 20
5.1 Informationssicherheitspolitik und -richtlinien ... 20
5.2 Informationssicherheitsrollen und -verantwortlichkeiten ... 22
5.3 Aufgabentrennung ... 23
5.4 Verantwortlichkeiten der Leitung ... 25
5.5 Kontakt mit Behörden ... 26
5.6 Kontakt mit speziellen Interessengruppen ... 27
5.7 Informationen über die Bedrohungslage ... 27
5.8 Informationssicherheit im Projektmanagement ... 29
5.9 Inventar der Informationen und anderer damit verbundener Werte ... 31
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten ... 33
5.11 Rückgabe von Werten ... 35
5.12 Klassifizierung von Informationen ... 36
5.13 Kennzeichnung von Informationen ... 38
5.14 Informationsübermittlung ... 39
5.15 Zugangssteuerung ... 42
5.16 Identitätsmanagement ... 45
5.17 Authentisierungsinformationen ... 46
5.18 Zugangsrechte ... 49
5.19 Informationssicherheit in Lieferantenbeziehungen ... 51
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen ... 53
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette ... 56
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen ... 58
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten ... 60
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen ... 63
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse ... 65
5.26 Reaktion auf Informationssicherheitsvorfälle ... 66
5.27 Erkenntnisse aus Informationssicherheitsvorfällen ... 67
5.28 Sammeln von Beweismaterial ... 68
5.29 Informationssicherheit bei Störungen ... 69
5.30 IKT-Bereitschaft für Business-Continuity ... 70
5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen ... 71
5.32 Geistige Eigentumsrechte ... 73

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

5.33 Schutz von Aufzeichnungen ... 75
5.34 Datenschutz und Schutz personenbezogener Daten (pbD) ... 77
5.35 Unabhängige Überprüfung der Informationssicherheit ... 78
5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit ... 79
5.37 Dokumentierte Betriebsabläufe ... 80

6 Personenbezogene Maßnahmen ... 82
6.1 Sicherheitsüberprüfung ... 82
6.2 Beschäftigungs- und Vertragsbedingungen ... 83
6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung ... 85
6.4 Maßregelungsprozess ... 87
6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung ... 88
6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ... 89
6.7 Remote-Arbeit ... 90
6.8 Meldung von Informationssicherheitsereignissen ... 92

7 Physische Maßnahmen ... 93
7.1 Physische Sicherheitsperimeter ... 93
7.2 Physischer Zutritt ... 94
7.3 Sichern von Büros, Räumen und Einrichtungen ... 96
7.4 Physische Sicherheitsüberwachung ... 97
7.5 Schutz vor physischen und umweltbedingten Bedrohungen ... 98
7.6 Arbeiten in Sicherheitsbereichen ... 100
7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren ... 101
7.8 Platzierung und Schutz von Geräten und Betriebsmitteln ... 102
7.9 Sicherheit von Werten außerhalb der Räumlichkeiten ... 103
7.10 Speichermedien ... 104
7.11 Versorgungseinrichtungen ... 106
7.12 Sicherheit der Verkabelung ... 107
7.13 Instandhaltung von Geräten und Betriebsmitteln ... 108
7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln ... 109

8 Technologische Maßnahmen ... 111
8.1 Endpunktgeräte des Benutzers ... 111
8.2 Privilegierte Zugangsrechte ... 113
8.3 Informationszugangsbeschränkung ... 115
8.4 Zugriff auf den Quellcode ... 117
8.5 Sichere Authentisierung ... 118
8.6 Kapazitätssteuerung ... 120
8.7 Schutz gegen Schadsoftware ... 122
8.8 Handhabung von technischen Schwachstellen ... 124
8.9 Konfigurationsmanagement ... 128
8.10 Löschung von Informationen ... 130
8.11 Datenmaskierung ... 132
8.12 Verhinderung von Datenlecks ... 134
8.13 Sicherung von Informationen ... 135
8.14 Redundanz von informationsverarbeitenden Einrichtungen ... 137
8.15 Protokollierung ... 138
8.16 Überwachung von Aktivitäten ... 142
8.17 Uhrensynchronisation ... 144
8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten ... 145
8.19 Installation von Software auf Systemen in Betrieb ... 146
8.20 Netzwerksicherheit ... 148
8.21 Sicherheit von Netzwerkdiensten ... 149
8.22 Trennung von Netzwerken ... 150
8.23 Webfilterung ... 152
8.24 Verwendung von Kryptographie ... 153

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

8.25 Lebenszyklus einer sicheren Entwicklung ... 155
8.26 Anforderungen an die Anwendungssicherheit ... 156
8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze ... 159
8.28 Sichere Codierung ... 161
8.29 Sicherheitsprüfung bei Entwicklung und Abnahme ... 164
8.30 Ausgegliederte Entwicklung ... 166
8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen ... 167
8.32 Änderungssteuerung ... 169
8.33 Testdaten ... 170
8.34 Schutz der Informationssysteme während Tests im Rahmen von Audits ... 171

Anhang A (informativ) Verwendung von Attributen ... 173
A.1 Allgemeines ... 173
A.2 Organisatorische Sichten ... 191

Anhang B (informativ) Übereinstimmung von ISO/IEC 27002:2022 (dieses Dokument) mit ISO/IEC 27002:2013 ... 193

Literaturhinweise ... 201

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 EN ISO/IEC 27702:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Mai 2023, und etwaige entgegenstehende nationale Normen müssen bis Mai 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO/IEC 27002:2017.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 vollständigen Zusammenhänge können Anhang B entnommen werden.

Diese korrigierte Version von 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 „#Vertrauenswürdigkeit_in_Bezug_auf_Informationssicherheit“ 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 Informationssicherheitsmanagementsystem (ISMS) auf der Grundlage von ISO/IEC 27001 verwendet werden. Es kann auch als Anleitung 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 ihres Managements und Betriebs, 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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) die Grundsätze, Ziele und Geschäftsanforderungen für alle Schritte des Lebenszyklus von Informationen, die eine Organisation zur Unterstützung ihrer Geschäftstätigkeit entwickelt hat.

0.3 Maßnahmen

Eine Aktivität, 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 Aktivitäten 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 „Anleitung“ und „Weitere Informationen“ in Abschnitt 5 bis Abschnitt 8 verwiesen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

1 Anwendungsbereich

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

a) im Rahmen eines Informationssicherheitsmanagementsystems (ISMS) auf der Basis von ISO/IEC 27001;

b) für die Umsetzung von Informationssicherheitsmaßnahmen auf der Grundlage international anerkannter bewährter Verfahren;

c) zur Entwicklung organisationsspezifischer Leitlinien 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
etwas, das 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;
  — Geschäfts*prozesse* (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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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
Nachweiskette
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
Maßnahme
Aktivität, durch die das Risiko beibehalten und/oder verändert wird

Anmerkung 1 zum Begriff: Maßnahmen 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: Maßnahmen können nicht immer die beabsichtigte oder angenommene verändernde Wirkung ausüben.

[QUELLE: ISO 31000:2018, 3.8]

3.1.9
Störung
Vorfall, 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: „Endpunktgerät“ kann 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

3.1.11
Entität
Element, das 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 Elemente, 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
Vorkommnis, das auf eine mögliche *Informationssicherheitsverletzung* (3.1.13) oder ein Versagen der *Maßnahmen* (3.1.8) hinweist

[QUELLE: ISO/IEC 27035-1:2016, 3.3, modifiziert — in der englischen Sprachfassung wurde „breach of information security“ durch „information security breach“ 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 deren Betrieb gefährden können

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

3.1.16
Handhabung von Informationssicherheitsvorfällen
Ausübung einer konsistenten und wirksamen Herangehensweise für den Umgang mit *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 Informationen bearbeitende Komponenten

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

3.1.18
interessierte Partei
Anspruchsgruppe
Person oder Organisation, die eine Entscheidung oder Tätigkeit beeinflussen, davon beeinflusst werden oder 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]

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

3.1.25
Datenschutz-Folgenabschätzung
DSFA
Gesamt*prozess* (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 wurde 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 zum Erzielen eines vorgesehenen Ergebnisses verwendet

[QUELLE: ISO 9000:2015, 3.4.1, modifiziert — die Anmerkungen zum Begriff wurden 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 wurde 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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

3.1.32
Regel
anerkannter Grundsatz oder Anweisung, der/die die Erwartungen der Organisation in Bezug auf das, was getan werden muss, erlaubt ist 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 Vorfalls, 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 Gegenstand 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
Benutzerendpunktgerät
Endpunktgerät (3.1.10), das von Benutzern für den Zugriff auf Informationsverarbeitungsdienste verwendet wird

Anmerkung 1 zum Begriff: „Endpunktgerät des Benutzers“ kann 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]

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

3.2 Abkürzungen

ABAC	attributbasierte Zugangssteuerung (en: attribute-based access control)
ACL	Zugangssteuerungsliste (en: access control list)
BIA	Analyse der geschäftlichen Auswirkungen (en: business impact analysis)
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 Zugangssteuerung (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 Zugangssteuerung (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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

RBAC	rollenbasierte Zugangssteuerung (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	drahtloser Netzwerkzugang (WLAN) (en: wireless fidelity)

4 Aufbau dieses Dokuments

4.1 Abschnitte

Dieses Dokument ist wie folgt strukturiert:

a) Organisatorische Maßnahmen (Abschnitt 5);

b) Personenbezogene Maßnahmen (Abschnitt 6);

c) Physische Maßnahmen (Abschnitt 7);

d) Technologische Maßnahmen (Abschnitt 8).

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

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

   Das Attribut „Maßnahmenart“ dient dazu, Maßnahmen unter dem Gesichtspunkt zu betrachten, 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

   Das Attribut „Informationssicherheitseigenschaften“ dient dazu, Maßnahmen unter dem Gesichtspunkt zu betrachten, welches Merkmal der Informationen durch die Maßnahme geschützt werden soll. Die Attributwerte bestehen aus Vertraulichkeit, Integrität und Verfügbarkeit.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

c) Cybersicherheitskonzepte

Das Attribut „Cybersicherheitskonzepte“ dient dazu, Maßnahmen unter dem Gesichtspunkt 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, Maßnahmen aus der Perspektive der Praxis 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, Aufrechterhaltung, Sicherheit_in_Lieferantenbeziehungen, Recht_und_Compliance, Handhabung_von_Informationssicherheitsereignissen und Vertrauenswürdigkeit_in_Bezug_auf_die_Informationssicherheit.

e) Sicherheitsdomänen

Sicherheitsdomänen ist ein Attribut, um Maßnahmen aus der Perspektive von vier Informationssicherheitsdomänen zu betrachten: „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;

— **Anleitung:** Wie die Maßnahme umgesetzt werden sollte;

— **Weitere Informationen:** Erläuternder Text oder Verweisungen auf andere einschlägige Dokumente.

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

5 Organisatorische Maßnahmen

5.1 Informationssicherheitspolitik und -richtlinien

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebs-fähigkeit	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.

Anleitung

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 Benutzerendpunktgeräten;

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 bei Folgendem umfassen:

a) der Geschäftsstrategie des Unternehmens;

b) dem technischen Umfeld der Organisation;

c) Vorschriften, Satzungen, Gesetze und Verträge;

d) Informationssicherheitsrisiken;

e) dem aktuellen und voraussichtlichen Bedrohungsumfeld der Informationssicherheit;

f) Lehren aus Informationssicherheitsereignissen und -vorfällen im Bereich der Informationssicherheit.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

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 sollten 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 Richtliniendokumente 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 anders 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	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebs-fähigkeit	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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Anleitung

Die Zuweisung von Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sollte in Übereinstimmung mit der Informationssicherheitspolitik und den themenspezifischen Richtlinien erfolgen (siehe 5.1). Die Organisation sollte Verantwortlichkeiten 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 rechenschaftspflichtig 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 Rolle 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 Aufgabentrennung

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Governance #Identitäts-_und_Zugangsverwaltung	#Governance_und_Ökosystem

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

Maßnahme

Sich widersprechende Aufgaben und Verantwortungsbereiche sollten voneinander getrennt werden.

Zweck

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

Anleitung

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

5.4 Verantwortlichkeiten der Leitung

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebs-fähigkeit	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 die Leitung ihre Rolle im Bereich der Informationssicherheit versteht und Schritte ergreift, die sicherstellen, dass das gesamte Personal seiner Verantwortung für die Informationssicherheit nachkommt.

Anleitung

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:

a) über seine Rollen und Verantwortlichkeiten in der Informationssicherheit informiert wird, bevor es Zugang zu den Informationen der Organisation und anderen damit verbundenen Werten erhält;

b) Leitlinien erhält, die die Erwartungen an seine Rolle in der Informationssicherheit innerhalb der Organisation darlegen;

c) den Auftrag hat, der Informationssicherheitspolitik und den themenspezifischen Richtlinien der Organisation gerecht zu werden;

d) ein Informationssicherheitsbewusstsein erreicht, das seinen Rollen und Verantwortlichkeiten in der Organisation entspricht (siehe 6.3);

e) Einhaltung der Beschäftigungsbedingungen, des Vertrages oder der Vereinbarung, einschließlich der Informationssicherheitspolitik der Organisation und geeigneter Arbeitsmethoden;

f) fortwährend durch ständige berufliche Weiterbildung angemessene Fähigkeiten und Qualifikationen im Bereich der Informationssicherheit besitzt ;

g) soweit praktikabel, über einen vertraulichen Kanal Verletzungen gegen die Informationssicher-heitspolitik, 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;

h) über angemessene Ressourcen und Projektplanungszeit für die Implementierung der sicherheits-relevanten Prozesse und Maßnahmen in der Organisation verfügt.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

Weitere Informationen

Keine weiteren Informationen.

5.5 Kontakt mit Behörden

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebs-fähigkeit	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 Justiz-, Regulierungs- und Aufsichtsbehörden.

Anleitung

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

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 Informationssicherheits-vorfällen (siehe 5.24 bis 5.28) oder für den Notfallplanungsprozess und den Prozess zur Business-Continuity (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)].

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

5.6 Kontakt mit speziellen Interessengruppen

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

Maßnahme

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

Zweck

Sicherstellung eines angemessenen Informationsflusses in Bezug auf die Informationssicherheit.

Anleitung

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

a) die Kenntnis über beste Praktiken zu verbessern und über relevante Sicherheitsinformationen auf dem Laufenden zu bleiben;

b) sicherzustellen, dass das Verständnis des Informationssicherheitsumfeldes aktuell ist;

c) rechtzeitig Warnungen, Hinweise und Patches zum Schutz vor Angriffen und Schwachstellen zu erhalten;

d) Zugang zu Fachberatung über Informationssicherheit zu erhalten;

e) Informationen über neue Technologien, Produkte, Dienste, Bedrohungen oder Schwachstellen auszutauschen;

f) geeignete Verbindungsstellen beim Umgang mit Informationssicherheitsvorfällen zu bieten (siehe 5.24 bis 5.28).

Weitere Informationen

Keine weiteren Informationen.

5.7 Informationen über die Bedrohungslage

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheits-domänen
#Präventiv #Detektiv #Korrektiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren #Erkennen #Reagieren	#Bedrohungs_und_Schwachstellenmanagement	#Verteidigung #Resilienz

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Maßnahme

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

Zweck

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

Anleitung

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

a) fundierte Schritte zu erleichtern, um zu verhindern, dass die Bedrohungen der Organisation Schaden zufügen;

b) die Auswirkungen solcher Bedrohungen zu verringern.

Informationen über die Bedrohungslage lassen sich in drei Schichten unterteilen, die alle berücksichtigt werden sollten:

a) strategische Bedrohungsanalyse: Austausch von High-Level-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.

Informationen über die Bedrohungslage sollten Folgendes sein:

a) relevant (d. h. im Zusammenhang mit dem Schutz der Organisation);

b) aufschlussreich (d. h. der Organisation ein genaues und detailliertes Verständnis der Bedrohungslandschaft vermitteln);

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 der Bedrohungsanalyse;

b) Ermittlung, Sicherheitsüberprüfung und Auswahl interner und externer Informationsquellen, die erforderlich und geeignet sind, um die für die Erstellung der Bedrohungslage 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);

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 über die Bedrohungslage 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, IDS 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 Informationen über die Bedrohungslage insgesamt zu verbessern.

Weitere Informationen

Organisationen können Bedrohungsdaten nutzen, um Bedrohungen zu verhindern, zu erkennen oder darauf zu reagieren. Organisationen können Bedrohungsdaten selbst erstellen, sie 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	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebs-fähigkeit	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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Anleitung

Die Informationssicherheit sollte in das Projektmanagement integriert werden, um sicherzustellen, dass die Risiken für die 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 mit der Durchführung von Projekten verbundenen Informationssicherheitsrisiken, wie z. B. die Sicherheit der internen und externen Kommunikationsaspekte während des gesamten Projektlebenszyklus berücksichtigt und behandelt werden;

d) die Fortschritte bei der Behandlung von Informationssicherheitsrisiken überprüft werden und die Wirksamkeit der Behandlung bewertet und geprüft wird.

Die Angemessenheit der Überlegungen und Aktivitäten zur Informationssicherheit sollte in festgelegten Phasen von geeigneten Personen oder Leitungsgremien wie dem Projektlenkungsausschuss 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 bestimmt werden, nicht nur für IKT-Entwicklungsprojekte. Bei der Bestimmung dieser Anforderungen sollten auch die folgenden Punkte berücksichtigt werden:

a) um welche Informationen es sich handelt (Informationsbestimmung), welche Informationssicherheits-erfordernisse 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 Authentisierung;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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) das Informieren 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 der 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 eine Anleitung zur Anwendung von Risikomanagement-Prozessen für die Ermittlung von Sicherheitsmaßnahmen zur Einhaltung der Informationssicherheitsanforderungen.

5.9 Inventar der Informationen und anderer damit verbundener Werte

Maßnahmenart	Informationssicher-heitseigenschaften	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 Werte, einschließlich der Eigentümer, sollte erstellt und gepflegt werden.

Zweck

Identifizierung der Informationen und anderen damit verbundenen Werte der Organisation, um deren Informationssicherheit zu wahren und entsprechende Zuständigkeiten zuzuweisen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

Anleitung

Inventar

Die Organisation sollte ihre Informationen und anderen damit verbundenen Werte identifizieren und deren Bedeutung in Bezug auf die Informationssicherheit bestimmen. Die Dokumentation sollte wie jeweils angemessen in eigenen oder bestehenden Inventaren aufbewahrt werden.

Das Inventar der Informationen und anderen damit verbundenen 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 damit verbundenen Werten gehören:

a) Durchführung regelmäßiger Überprüfungen der identifizierten Informationen und anderen damit verbundenen Werten anhand des Inventars der Werte;

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 braucht nicht eine einzige Liste von Informationen und anderen damit verbundenen Werten zu sein. In Anbetracht der Tatsache, dass das Inventar von den betreffenden 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 der Informationen und anderen damit verbundenen Werte 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 anderen damit verbundenen 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 Zuweisung 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;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

e) Anforderungen für den zulässigen Gebrauch von Informationen und anderen damit verbundenen Werten (siehe 5.10) festgelegt werden;

f) die Zugangsbeschränkungen der Klassifizierung entsprechen, wirksam sind und regelmäßig überprüft werden;

g) Informationen und andere damit verbundene Werte, wenn sie gelöscht oder entsorgt werden, auf sichere Weise gehandhabt und aus dem Inventar entfernt werden;

h) er an der Identifizierung und dem Management der mit seinem/seinen Wert(en) verbundenen Risiken beteiligt ist;

i) er das Personal unterstützt, das die Aufgabe und die Verantwortung hat, ihre Informationen zu verwalten.

Weitere Informationen

Inventare von Informationen und anderen damit verbundenen Werten sind oft notwendig, um den wirksamen Schutz von Informationen sicherzustellen, und können auch für andere Zwecke erforderlich sein, z. B. für Gesundheit und Sicherheit, Versicherung oder aus finanziellen Gründen. Die Inventare von Informationen und anderen damit verbundenen 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 damit verbundenen Werten zu benennen, die bei der Erbringung einer bestimmten Dienstleistung zusammenwirken. In diesem Fall ist der Zuständige für diese Dienstleistung für deren Erbringung rechenschaftspflichtig, 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	Informationssicher-heitseigenschaften	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 damit verbundenen Werten 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

Anleitung

Personal und sonstige Benutzer, die zu externen Parteien gehören, die Informationen und andere damit verbundene Werte der Organisation nutzen oder Zugriff darauf haben, sollten auf die Informationssicherheitsanforderungen zum Schutz und zur Handhabung der Informationen und anderen damit verbundenen Werten der Organisation hingewiesen werden. Sie sollten für ihre eigene Nutzung informationsverarbeitender Einrichtungen verantwortlich sein.

Die Organisation sollte eine themenspezifische Richtlinie für die zulässige Nutzung von Informationen und anderen zugehörigen Vermögenswerten aufstellen und sie an alle Personen weitergeben, die Informationen und andere damit verbundene Werte nutzen oder bearbeiten. Die themenspezifische Richtlinie über den zulässigen Gebrauch sollte klare Anweisungen darüber geben, wie Einzelpersonen Informationen und andere damit verbundene Werte nutzen sollen. Die themenspezifische Richtlinie sollte Folgendes 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 deren 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 physisch) als Hinweis für den berechtigten Empfänger (siehe 7.10);

f) Genehmigung der Entsorgung von Informationen und anderen damit verbundenen 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 gesteuert werden, beispielsweise durch Vereinbarungen mit Cloud-Service-Anbietern. Mit Vorsicht sollte auch vorgegangen werden, wenn eine kollaborative Arbeitsumgebung genutzt wird.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

5.11 Rückgabe von Werten

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

Maßnahme

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

Zweck

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

Anleitung

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 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 Personal 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 Informationen (z. B. geistiges Eigentum) durch das gekündigte Personal verhindern.

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

a) Endpunktgeräte des Benutzers;

b) tragbare Speichergeräte;

c) Spezialausrüstung;

d) Authentisierungshardware (z. B. mechanische Schlüssel, physische Token und Smartcards) für Informationssysteme, Standorte und physische Archive;

e) physische Kopien von Informationen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 Informationen

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Identifizieren	#Informationsschutz	#Schutz #Verteidigung

Maßnahme

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

Zweck

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

Anleitung

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.

Klassifizierungen und damit verbundene Schutzmaßnahmen für Informationen sollten geschäftlichen Erfordernissen der gemeinsamen Nutzung oder der Einschränkung von Informationen, des Schutzes der Integrität von Informationen und der Sicherstellung der Verfügbarkeit sowie rechtlichen Anforderungen an die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen Rechnung tragen. Werte, bei denen es sich nicht um Informationen handelt, können auch unter Einhaltung der Klassifizierung der im Wert gespeicherten, durch diesen verarbeiteten oder auf andere Weise gehandhabten oder geschützten Informationen klassifiziert werden.

Die Zuständigen für die Informationen sollten für deren Klassifizierung rechenschaftspflichtig 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 der Kritikalität 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 sinnvoll ist.

Das Schema sollte innerhalb der gesamten Organisation einheitlich sein und in deren 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 Einrichtung 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.

Informationen können ihren sensiblen oder kritischen Charakter nach einer gewissen Zeitspanne verlieren. Wenn die Informationen beispielsweise öffentlich zugänglich gemacht wurden, gelten keine Anforderungen mehr an ihre Vertraulichkeit, aber ihre Integrität und Verfügbarkeit müssen möglicherweise 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. Umgekehrt kann eine Unterklassifizierung zu unzureichenden Maßnahmen zum Schutz der Informationen vor Kompromittierung führen.

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 auf Geschäftsziele;

d) Offenlegung hat schwerwiegende Auswirkungen auf langfristige Geschäftsziele und gefährdet den Bestand der Organisation.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

5.13 Kennzeichnung von Informationen

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Informationsschutz	#Verteidigung #Schutz

Maßnahme

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

Zweck

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

Anleitung

Verfahren zur Kennzeichnung von Informationen sollten Informationen 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 in Abhängigkeit vom jeweiligen Speichermedientyp auf die Informationen zugegriffen bzw. mit den Werten umgegangen wird. Die Verfahren können Folgendes festlegen:

a) Fälle, in denen auf eine Kennzeichnung verzichtet wird (z. B. bei nicht vertraulichen Informationen, um die Arbeitsbelastung zu verringern);

b) wie Informationen zu kennzeichnen sind, die auf elektronischem oder physischem Wege oder in einem anderen Format übermittelt oder gespeichert werden;

c) wie mit Fällen umzugehen ist, in denen eine Kennzeichnung nicht möglich ist (z. B. aufgrund technischer Beschränkungen).

Beispiele für Kennzeichnungsverfahren umfassen:

a) physische Kennzeichnungen;

b) Kopf- und Fußzeilen;

c) Metadaten;

d) Wasserzeichenmarkierung;

e) Stempel.

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 Systemen erleichtern, zu interagieren und Entscheidungen auf der Grundlage der zugehörigen Klassifizierungskennzeichnung zu treffen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

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 kritisch eingestufte Informationen enthalten, sollten eine entsprechende Klassifizierungskennzeichnung tragen.

Weitere Informationen

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

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

Die Kennzeichnung von Informationen und anderer damit verbundener 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 Informationsübermittlung

Maßnahmenart	Informationssicher-heitseigenschaften	Konzepte zur Cybersicherheit	Betriebsfähigkeit	Sicherheitsdomänen
#Präventiv	#Vertraulichkeit #Integrität #Verfügbarkeit	#Schützen	#Asset_Management #Informationsschutz	#Schutz

Maßnahme

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

Zweck

Aufrechterhaltung der Sicherheit übermittelter Informationen sowohl innerhalb einer Organisation als auch mit jeglicher externen interessierten Partei.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Anleitung

Allgemeines

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

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

Für alle Arten der Informationsübermittlung sollten Regeln, Verfahren und Vereinbarungen Folgendes beinhalten:

a) Maßnahmen zum Schutz der übermittelten 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 Nachweiskette für Informationen, während diese übermittelt werden;

c) Identifizierung geeigneter Kontaktpersonen für die Übermittlung, einschließlich der Verantwortlichen der Informationen, der Risikoverantwortlichen, der Sicherheitsbeauftragten und der Informationsverwalter, soweit zutreffend;

d) Verantwortlichkeiten und Haftung bei Informationssicherheitsvorfällen wie dem Verlust physischer Speichermedien oder Daten;

e) Verwendung eines vereinbarten Kennzeichnungssystems für sensible oder kritische Informationen, wobei sicherzustellen ist, dass die Kennzeichnungen ohne weiteres verständlich und die Informationen angemessen geschützt sind (siehe 5.13);

f) Zuverlässigkeit und Verfügbarkeit des Übermittlungsdienstes;

g) die themenspezifische Richtlinie oder die Leitlinien für die zulässige Nutzung von Einrichtungen zur Informationsübermittlung (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 Übermittlung von Informationen (z. B. Anforderungen an elektronische Signaturen).

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Elektronische Übermittlung

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

a) Erkennung von und Schutz vor Schadsoftware, die durch die Verwendung elektronischer Kommunikation übermittelt werden können (siehe 8.7);

b) Schutz übermittelter 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 Authentisierungsstufen bei der Übermittlung 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, en: short message service) 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.

Übermittlung physischer Speichermedien

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

a) Verantwortlichkeiten für die Steuerung von und Mitteilung bezüglich Übermittlung, 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 Kuriere, die von der Geschäftsleitung genehmigt wurde;

e) Standards zur Identifizierung eines Kurierunternehmens;

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

f) je nach Klassifizierungsgrad der Informationen in den zu transportierenden Speichermedien manipulationsaufzeigende oder manipulationssichere Maßnahmen (z. B. Taschen, Behälter) anwenden;

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 Übermittlung

Um die mündliche Übermittlung 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 als Sprachnachrichten, da diese von unbefugten Personen wiedergegeben, auf gemeinsamen Systemen gespeichert oder beim Wählen einer falschen Nummer ordnungswidrig gespeichert werden können;

c) auf die geeignete Lautstärke, wie notwendig, um das Gespräch zu verfolgen, abgeschirmt werden;

d) sicherstellen, dass geeignete Maßnahmen zu den Räumlichkeiten getroffen werden (z. B. Schallisolierung, geschlossene Türen);

e) alle sensiblen Gespräche mit einer Erklärung beginnen, sodass die Anwesenden die Klassifizierungsstufe dessen, was sie hören werden, kennen und wissen, welche Anforderungen an den Umgang mit dem Gehörten 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 Steuerung des physischen und logischen Zugriffs auf Informationen und andere damit verbundene Werte sollten auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01

Zweck

Sicherstellung des befugten Zugangs und Verhinderung des unbefugten Zugangs zu Informationen und anderen damit verbundenen Werten.

Anleitung

Die Zuständigen für Informationen und andere damit verbundene Werte sollten die Anforderungen an die Informationssicherheit und die Geschäftsanforderungen 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 damit verbundenen Werten benötigen;

b) Sicherheit der Anwendungen (siehe 8.26);

c) physischer Zugang, der durch geeignete physische Zutrittskontrollen 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 zu Daten oder Diensten (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;

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27002:2024-01

c) Berücksichtigung aller Arten von verfügbaren Verbindungen in verteilten Umgebungen, so dass Entitäten nur Zugang zu Informationen und anderen damit verbundenen Werten 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 Kenntnisanforderungen 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, 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 ausgelöst werden 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(e), 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 Zugangssteuerung, en: mandatory access control), DAC (benutzerbestimmbare Zugangssteuerung, en: discretionary access control), RBAC (rollenbasierte Zugangssteuerung, en: role-based access control) und ABAC (attributbasierte Zugangssteuerung, en: attribute-based access control).

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27002:2024-01