

DIN EN ISO/IEC 27010

ICS 03.100.70; 33.030

Einsprüche bis 2020-03-17

Entwurf

**Informationstechnik –
Sicherheitsverfahren –
Informationssicherheitsmanagement für sektor- und
organisationsübergreifende Kommunikation (ISO/IEC 27010:2015);
Deutsche und Englische Fassung prEN ISO/IEC 27010:2020**

Information technology –
Security techniques –
Information security management for inter-sector and inter-organizational communications
(ISO/IEC 27010:2015);
German and English version prEN ISO/IEC 27010:2020

Technologies de l'information –
Techniques de sécurité –
Gestion de la sécurité de l'information des communications intersectorielles et
interorganisationnelles (ISO/IEC 27010:2015);
Version allemande et anglaise prEN ISO/IEC 27010:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-01-17 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

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

Gesamtumfang 86 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27010:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27010:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

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

ISO/IEC 27001:2013 siehe DIN EN ISO/IEC 27001:2017-06

ISO/IEC 27002:2013 siehe DIN EN ISO/IEC 27002:2017-06

Nationaler Anhang NA (informativ)

Literaturhinweise

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 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

**Informationstechnik — Sicherheitsverfahren —
Informationssicherheitsmanagement für sektor- und
organisationsübergreifende Kommunikation (ISO/IEC 27010:2015)**

Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles (ISO/IEC 27010:2015)

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications (ISO/IEC 27010:2015)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Begriffe und Erläuterung	8
4.1 Einleitung	8
4.2 Informationsaustauschende Gemeinschaften	9
4.3 Verwaltung von Gemeinschaften	9
4.4 Unterstützende Stellen	9
4.5 Sektorübergreifende Kommunikation	10
4.6 Konformität	10
4.7 Kommunikationsmodell	11
5 Informationssicherheitsrichtlinien	12
5.1 Vorgaben der Leitung für Informationssicherheit	12
5.1.1 Informationssicherheitsrichtlinien	12
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	12
6 Organisation der Informationssicherheit	12
7 Personalsicherheit	12
7.1 Vor der Beschäftigung	12
7.1.1 Sicherheitsüberprüfung	12
7.1.2 Beschäftigungs- und Vertragsbedingungen	13
7.2 Während der Beschäftigung	13
7.3 Beendigung und Änderung der Beschäftigung	13
8 Verwaltung der Werte	13
8.1 Verantwortlichkeit für Werte	13
8.1.1 Inventarisierung der Werte	13
8.1.2 Zuständigkeit für Werte	13
8.1.3 Zulässiger Gebrauch von Werten	13
8.1.4 Rückgabe von Werten	13
8.2 Informationsklassifizierung	14
8.2.1 Klassifizierung von Informationen	14
8.2.2 Kennzeichnung von Informationen	14
8.2.3 Handhabung von Werten	14
8.3 Handhabung von Datenträgern	14
8.4 Schutz des Informationsaustauschs	15
8.4.1 Weitergabe von Informationen	15
8.4.2 Haftungsausschluss für Informationen	15
8.4.3 Glaubwürdigkeit von Informationen	16
8.4.4 Verringerung der Sensibilität von Informationen	16
8.4.5 Schutz von anonymen Quellen	16
8.4.6 Schutz von anonymen Empfängern	17

8.4.7	Berechtigung zur weiteren Weitergabe	17
9	Zugangssteuerung	17
10	Kryptographie	18
10.1	Kryptographische Maßnahmen	18
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	18
10.1.2	Schlüsselverwaltung	18
11	Physische und umgebungsbezogene Sicherheit	18
12	Betriebssicherheit.....	18
12.1	Betriebsabläufe und -verantwortlichkeiten.....	18
12.2	Schutz vor Schadsoftware.....	18
12.2.1	Maßnahmen gegen Schadsoftware	18
12.3	Datensicherung	18
12.4	Protokollierung und Überwachung.....	19
12.4.1	Ereignisprotokollierung	19
12.4.2	Schutz der Protokollinformation.....	19
12.4.3	Administratoren- und Bedienerprotokolle	19
12.4.4	Uhrensynchronisation.....	19
12.5	Steuerung von Software im Betrieb.....	19
12.6	Handhabung technischer Schwachstellen.....	19
12.7	Audits von Informationssystemen	19
12.7.1	Maßnahmen für Audits von Informationssystemen.....	19
12.7.2	Auditberechtigungen in der Gemeinschaft.....	19
13	Kommunikationssicherheit.....	20
13.1	Netzwerksicherheitsmanagement.....	20
13.2	Informationsübertragung	20
13.2.1	Richtlinien und Verfahren für die Informationsübertragung.....	20
13.2.2	Vereinbarungen zur Informationsübertragung.....	20
13.2.3	Elektronische Nachrichtenübermittlung.....	20
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	20
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	20
15	Lieferantenbeziehungen.....	21
15.1	Informationssicherheit in Lieferantenbeziehungen	21
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	21
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	21
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie.....	21
15.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	21
16	Handhabung von Informationssicherheitsvorfällen.....	21
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	21
16.1.1	Verantwortlichkeiten und Verfahren	21
16.1.2	Meldung von Informationssicherheitsereignissen	21
16.1.3	Meldung von Schwächen in der Informationssicherheit	22
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse.....	22
16.1.5	Reaktion auf Informationssicherheitsvorfälle	22
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	22
16.1.7	Sammeln von Beweismaterial	22
16.1.8	Frühwarnsystem.....	23
17	Informationssicherheitsaspekte beim Business Continuity Management	23
17.1	Aufrechterhalten der Informationssicherheit.....	23
17.1.1	Planung der Aufrechterhaltung der Informationssicherheit.....	23
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit.....	23
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	23

17.2	Redundanzen	23
18	Compliance.....	24
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen.....	24
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	24
18.1.2	Geistige Eigentumsrechte	24
18.1.3	Schutz von Aufzeichnungen	24
18.1.4	Privatsphäre und Schutz von personenbezogenen Informationen	24
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen	24
18.1.6	Haftung gegenüber der informationsaustauschenden Gemeinschaft	24
18.2	Überprüfungen der Informationssicherheit	25
Anhang A (informativ) Teilen von sensiblen Informationen		26
A.1	Einleitung	26
A.2	Herausforderungen	27
A.3	Möglicher Nutzen.....	28
A.4	Anwendbarkeit.....	28
A.5	Definition und Betrieb einer informationsaustauschenden Gemeinschaft	28
A.6	Vereinbarungen zum Informationsaustausch	30
A.7	Erfolgsfaktoren.....	31
A.8	Anwendungsbereich des ISMS für eine informationsaustauschende Gemeinschaft.....	31
Anhang B (informativ) Schaffen von Vertrauen in den Informationsaustausch.....		32
B.1	Vertrauen in Aussagen.....	32
B.2	Technologische Unterstützung.....	32
B.2.1	Einleitung	32
B.2.2	Anonymität und Pseudoanonymität.....	33
B.2.3	Reputations-Engines	34
B.3	Beurteilung der Vertrauenswürdigkeit von Informationen.....	35
Anhang C (informativ) Das Ampelprotokoll		38
Anhang D (informativ) Modelle für die Organisation einer informationsaustauschenden Gemeinschaft.....		39
D.1	Einleitung	39
D.2	Vertrauenswürdige Einheiten zur Informationsverbreitung (TICE)	39
D.2.1	Einleitung	39
D.2.2	Organisatorische Aspekte von TICE.....	40
D.2.3	Kerndienstleistungen und optionale Dienstleistungen einer TICE	41
D.2.4	Zusammenfassung.....	42
D.3	Warn-, Hinweis- und Meldestellen	42
D.3.1	Einleitung	42
D.3.2	Funktionen von WARPs.....	43
D.3.3	WARP-Dienstleistungen.....	43
D.3.4	Vorteile von WARPs.....	44
D.3.5	Zusammenfassung.....	45
Literaturhinweise.....		46

Europäisches Vorwort

Der Text von ISO/IEC 27010:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27010:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27010:2015 wurde von CEN als prEN ISO/IEC 27010:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

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).

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).

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

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword - Supplementary information.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques*, erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27010:2012), die aus Gründen der Kompatibilität mit ISO/IEC 27001:2013 und ISO/IEC 27002:2013 technisch überarbeitet wurde.

Einleitung

Diese Internationale Norm ist eine branchenspezifische Ergänzung zu ISO/IEC 27001:2013 und ISO/IEC 27002:2013 für die Anwendung durch informationsaustauschende Gemeinschaften. Die in dieser Internationalen Norm enthaltenen Leitlinien ergänzen die allgemeinen Leitlinien, die in anderen Teilen der Normenreihe ISO/IEC 27000 enthalten sind.

ISO/IEC 27001:2013 und ISO/IEC 27002:2013 behandeln den Informationsaustausch zwischen Organisationen, jedoch auf allgemeine Weise. Wenn Organisationen sensible Informationen an mehrere andere Organisationen weitergeben möchten, muss der Absender darauf vertrauen können, dass bei deren Verwendung in den anderen empfangenden Organisationen angemessene Sicherheitsmaßnahmen bestehen. Dies kann durch die Einrichtung einer informationsaustauschenden Gemeinschaft erreicht werden, in der jedes Mitglied den anderen Mitgliedern dahingehend vertraut, dass sie die gemeinsamen Informationen schützen, auch wenn die Organisationen sonst möglicherweise in Konkurrenz zueinander stehen.

Eine informationsaustauschende Gemeinschaft kann nicht ohne Vertrauen funktionieren. Die Bereitsteller von Informationen müssen darauf vertrauen können, dass die Empfänger die Daten nicht offenlegen oder sie für unangemessene Maßnahmen nutzen. Die Empfänger von Informationen müssen darauf vertrauen können, dass die Informationen korrekt sind, vorbehaltlich der vom Absender mitgeteilten Qualifikationen. Beide Aspekte sind wichtig und müssen durch nachweislich wirksame Sicherheitsrichtlinien und die Anwendung bewährter Verfahren unterstützt werden. Um dies zu erreichen, müssen die Mitglieder der Gemeinschaft alle ein gemeinsames Managementsystem einführen, das die Sicherheit der gemeinsamen Informationen abdeckt. Dabei handelt es sich um ein Informationssicherheitsmanagementsystem (ISMS) für die informationsaustauschende Gemeinschaft.

Darüber hinaus kann ein Informationsaustausch zwischen informationsaustauschenden Gemeinschaften stattfinden, wobei dem Absender nicht alle Empfänger bekannt sind. Dies wird nur funktionieren, wenn ein angemessenes Vertrauen zwischen den Gemeinschaften und in deren Vereinbarungen über den Informationsaustausch besteht. Es ist besonders wichtig für den Austausch sensibler Informationen zwischen verschiedenen Gemeinschaften, wie z. B. verschiedenen Branchen oder Marktsektoren.

1 Anwendungsbereich

Diese Internationale Norm enthält ergänzend zu den Leitlinien der Normenfamilie ISO/IEC 27000 Leitlinien zur Umsetzung des Informationssicherheitsmanagements in informationsaustauschenden Gemeinschaften.

Zudem enthält diese Internationale Norm spezifische Maßnahmen und Leitlinien zum Einführen, Umsetzen, Aufrechterhalten und Verbessern der Informationssicherheit bei der Kommunikation zwischen Organisationen und Sektoren. Sie enthält Leitlinien und allgemeine Grundsätze dazu, wie die festgelegten Anforderungen mit Hilfe von etablierten nachrichtentechnischen und weiteren technischen Methoden erfüllt werden können.

Diese Internationale Norm gilt für alle Formen des Austauschs und des Teilens sensibler Informationen, sowohl öffentlich als auch privat, national wie international, innerhalb derselben Branche oder desselben Marktsektors bzw. zwischen Branchen oder Sektoren. Insbesondere kann sie für den Austausch und das Teilen von Informationen in Bezug auf die Bereitstellung, Instandhaltung und den Schutz der kritischen Infrastruktur einer Organisation oder eines Nationalstaates gelten. Sie soll Vertrauen beim Austausch und dem Teilen sensibler Informationen schaffen und so das internationale Wachstum von informationsaustauschenden Gemeinschaften fördern.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000:2014.

4 Begriffe und Erläuterung

4.1 Einleitung

In Abschnitt 5 bis Abschnitt 18 dieser Internationalen Norm wurden ISMS-Leitlinien speziell für die sektor- und organisationsübergreifende Kommunikation festgelegt.

ISO/IEC 27002:2013 definiert Maßnahmen, die den Informationsaustausch zwischen Organisationen auf bilateraler Basis abdecken, sowie Maßnahmen für die allgemeine Weitergabe öffentlich zugänglicher Informationen. Unter bestimmten Umständen besteht jedoch die Notwendigkeit, Informationen innerhalb einer Gemeinschaft von Organisationen auszutauschen, bei denen die Informationen in gewisser Weise sensibel sind und nicht öffentlich zugänglich gemacht werden können, außer den Mitgliedern der Gemeinschaft. Häufig können die Informationen nur bestimmten Personen innerhalb jeder Mitgliedsorganisation zugänglich gemacht werden, oder es können andere Sicherheitsanforderungen wie die Anonymisierung von Informationen bestehen. Diese Internationale Norm definiert zusätzliche potenzielle

Maßnahmen und enthält zusätzliche Leitlinien und Interpretationen von ISO/IEC 27001:2013 und ISO/IEC 27002:2013, um diese Anforderungen zu erfüllen.

Es gibt vier informative Anhänge. Anhang A beschreibt die potenziellen Vorteile des Teilens sensibler Informationen zwischen Organisationen. Anhang B enthält Leitlinien dazu, wie Mitglieder einer informationsaustauschenden Gemeinschaft das Vertrauen in die von anderen Mitgliedern bereitgestellten Informationen bewerten können. Anhang C beschreibt das Ampelprotokoll, einen in informationsaustauschenden Gemeinschaften weit verbreiteten Mechanismus zur Angabe der zulässigen Weitergabe von Informationen. Anhang D enthält einige Beispiele für Modelle zur Organisation einer informationsaustauschenden Gemeinschaft.

4.2 Informationsaustauschende Gemeinschaften

Um effektiv zu sein, müssen informationsaustauschende Gemeinschaften ein gemeinsames Interesse haben oder in einer anderen Beziehung zueinander stehen, um den Umfang der geteilten sensiblen Informationen zu definieren. So können beispielsweise Gemeinschaften spezifisch für Marktsektoren sein und die Mitgliedschaft auf Organisationen innerhalb dieses Sektors beschränken. Natürlich kann es auch andere Grundlagen für das gemeinsame Interesse geben, z. B. den geografischen Standort oder das gemeinsame Eigentum.

Es muss auch Vertrauen unter den Mitgliedern bestehen, insbesondere dahingehend, dass alle Mitglieder die Vereinbarung über das Teilen von Informationen einhalten.

4.3 Verwaltung von Gemeinschaften

Informationsaustauschende Gemeinschaften werden von unabhängigen Organisationen oder Teilen von Organisationen gegründet. Daher sind möglicherweise nicht immer klare oder einheitliche Organisationsstrukturen und Verwaltungsfunktionen vorhanden, die für alle Mitglieder gelten. Für eine effektive Verwaltung der Informationssicherheit ist ein entsprechendes Bekenntnis erforderlich. Daher sollten die für die Verwaltung der Sicherheit von gemeinschaftlichen Informationen geltenden Organisationsstrukturen und Verwaltungsfunktionen klar definiert werden.

Unterschiede zwischen den Mitgliedsorganisationen einer informationsaustauschenden Gemeinschaft sollten ebenfalls berücksichtigt werden. Bei diesen Unterschieden könnte es sich um Folgendes handeln:

- unterschiedliche rechtliche oder regulatorische Rahmenbedingungen;
- Betrieb von eigenen ISMS innerhalb von Mitgliedsorganisationen;
- Regeln von Mitgliedern über den Schutz von Werten und die Offenlegung von Informationen.

4.4 Unterstützende Stellen

Viele informationsaustauschende Gemeinschaften werden sich dafür entscheiden, eine zentrale unterstützende Stelle einzurichten oder zu ernennen, die das Teilen von Informationen organisiert und unterstützt. Eine solche Stelle kann viele unterstützende Maßnahmen, z. B. die Anonymisierung von Quelle und Empfängern, einfacher und effizienter ergreifen als dies bei der direkten Kommunikation unter den Mitgliedern der Fall wäre.

Es gibt eine Reihe von verschiedenen Organisationsmodellen, die zum Aufbau von unterstützenden Stellen verwendet werden können. Anhang D beschreibt zwei gebräuchliche Modelle: die vertrauenswürdige Einheit zur Informationsverbreitung (en: Trusted Information Communication Entity, TICE) und die Warn-, Hinweis- und Meldestelle (en: Warning, Advice and Reporting Point, WARP).

4.5 Sektorübergreifende Kommunikation

Viele informationsaustauschende Gemeinschaften werden sektorbezogen sein, da Sektoren einen natürlichen Bereich von gemeinsamen Interessen darstellen. Es kann jedoch durchaus Informationen geben, die innerhalb solcher Gemeinschaften geteilt werden, die auch für andere in anderen Sektoren ansässige Gemeinschaften von Interesse sind. In solchen Fällen können informationsaustauschende Gemeinschaften bestehend aus informationsaustauschenden Gemeinschaften eingerichtet werden, die ebenfalls auf einem gemeinsamen Interesse, wie beispielsweise der Art der geteilten Informationen, basieren können. Diese wird als sektorübergreifende Kommunikation bezeichnet.

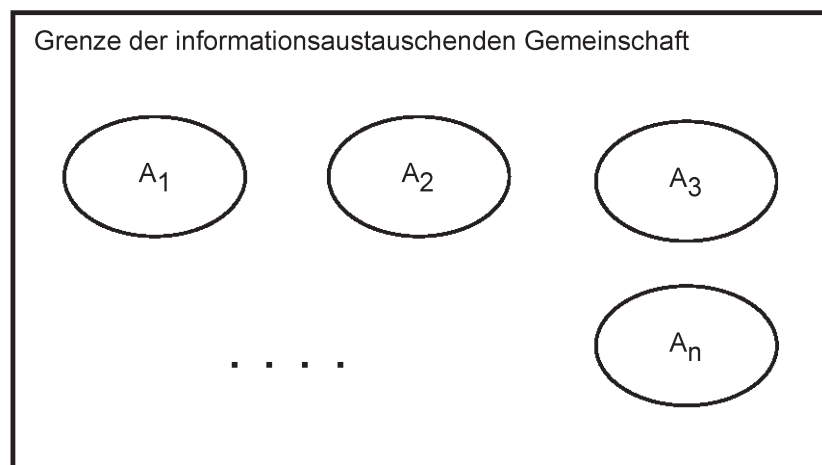
Die sektorübergreifende Kommunikation wird erheblich erleichtert, wenn unterstützende Stellen innerhalb jeder informationsaustauschenden Gemeinschaft vorhanden sind, da die notwendigen Vereinbarungen und Maßnahmen zum Informationsaustausch dann zwischen den unterstützenden Stellen und nicht zwischen allen Mitgliedern aller Gemeinschaften getroffen werden können. Einige sektorübergreifenden Gemeinschaften werden eine Anonymisierung der Quell- oder Empfängerorganisationen erfordern. Dies kann auch durch den Einsatz von unterstützenden Stellen erreicht werden.

4.6 Konformität

In gewissen Bereichen muss die Norm ISO/IEC 27001:2013 beim Anwenden auf eine informationsaustauschende Gemeinschaft (oder, bei sektorübergreifender Kommunikation, auf eine Gemeinschaft aus Gemeinschaften) interpretiert werden.

Der erste Bereich, in dem eine Interpretation erforderlich ist, ist die Definition der betreffenden Organisation.

Nach ISO/IEC 27001:2013 wird die Einrichtung, Implementierung, Pflege und kontinuierliche Verbesserung eines ISMS durch eine Organisation gefordert (ISO/IEC 27001:2013, 4.4). In diesem Zusammenhang handelt es sich bei der Organisation um die informationsaustauschende Gemeinschaft. Die Mitglieder der informationsaustauschenden Gemeinschaft werden jedoch selbst Organisationen sein – siehe Bild 1.



Legende

A_k Mitgliedsorganisation k der Gemeinschaft (k = 1 ... n), einschließlich jeglicher unterstützenden Stelle.

Bild 1 — Gemeinschaften und Organisationen

Zweitens wird in vielen informationsaustauschenden Gemeinschaften nicht allen Personen innerhalb der Mitgliedsorganisationen der Zugang zu den sensiblen Informationen gewährt, die zwischen den Mitgliedern ausgetauscht werden. In diesem Fall wird ein Teil der Mitgliedsorganisation innerhalb des Anwendungsbereichs des ISMS der Gemeinschaft liegen und ein Teil außerhalb. Der Teil außerhalb des Anwendungsbereichs

bereichs der Gemeinschaft hat nur dann Zugriff auf Gemeinschaftsinformationen, wenn sie für eine weiter gefasste Veröffentlichung gekennzeichnet sind – siehe Bild 2.

Die Mitglieder der informationsaustauschenden Gemeinschaft verfügen möglicherweise über eigene Informationssicherheitsmanagementsysteme, sodass einige Prozesse möglicherweise sowohl in den Anwendungsbereich der Gemeinschaft als auch in den Anwendungsbereich der Managementsysteme der Mitglieder fallen können. In diesem Fall besteht zumindest die theoretische Möglichkeit, dass es widersprüchliche und inkompatible Anforderungen an diese Prozesse geben könnte. Ein Problem könnte z. B. darin bestehen, den Ausschluss aus dem Anwendungsbereich des ISMS des Mitglieds zu rechtfertigen – siehe ISO/IEC 27001:2013, 4.3.

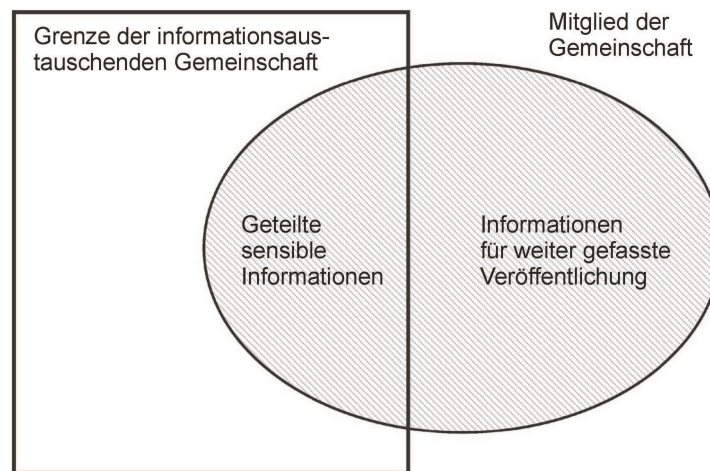


Bild 2 — Teilweise innerhalb des Anwendungsbereichs liegendes ISMS eines Mitglieds

Bei der Definition ihres Risikobeurteilungsprozesses (ISO/IEC 27001:2013, 6.1.2) muss die informationsaustauschende Gemeinschaft erkennen, dass die Auswirkungen von Risiken auf verschiedene Mitglieder der Gemeinschaft unterschiedlich sein können. Die Gemeinschaft wird sich daher für eine Risikobeurteilungsmethodik entscheiden müssen, in der uneinheitliche Auswirkungen berücksichtigt werden können. Gleiches gilt für die Kriterien zur Risikobeurteilung.

4.7 Kommunikationsmodell

Die Kommunikation sensibler Informationen nach dieser Internationalen Norm kann in jeder Form – schriftlich, mündlich oder elektronisch – erfolgen, vorausgesetzt, die ausgewählten Kontrollanforderungen werden erfüllt.

Im weiteren Verlauf dieser Internationalen Norm wird die individuelle sensible Kommunikation in Bezug auf die folgenden Teilnehmer beschrieben.

- Die *Quelle* einer Information ist die Person oder Organisation, die eine Information hervorbringt; die Quelle muss nicht Mitglied der Gemeinschaft sein.
- Der *Absender* ist Mitglied einer informationsaustauschenden Gemeinschaft, der ihre Weitergabe innerhalb der Gemeinschaft initiiert. Der Absender kann die Informationen direkt weitergeben oder zur Weitergabe an eine unterstützende Stelle senden. Der Absender kann, muss aber nicht, gleichzeitig die Quelle der Informationen sein; der Absender darf die Identität der Quelle verbergen. Die Gemeinschaften dürfen Vorkehrungen bereitstellen, mit denen Mitglieder ihre eigene Identität als Absender verbergen können.
- Ein *Empfänger* ist ein Empfänger von Informationen, die innerhalb der Gemeinschaft weitergegeben werden. Die Empfänger müssen nicht Mitglied der Gemeinschaft sein, wenn die Informationen als für

eine weiter gefasste Weitergabe verfügbar gekennzeichnet werden. Die Gemeinschaften dürfen Vorkehrungen bereitstellen, mit denen Empfänger ihre Identität vor den Absendern von Informationen verbergen können.

5 Informationssicherheitsrichtlinien

5.1 Vorgaben der Leitung für Informationssicherheit

5.1.1 Informationssicherheitsrichtlinien

ISO/IEC 27002:2013, Maßnahme 5.1.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Eine Richtlinie für den Informationsaustausch sollte festlegen, wie die Mitglieder der Gemeinschaft zusammenarbeiten werden, um Richtlinien für das Sicherheitsmanagement und die Ausrichtung der informationsaustauschenden Gemeinschaft zu definieren. Sie sollte allen Mitarbeitern zur Verfügung gestellt werden, die am Informationsaustausch innerhalb der Gemeinschaft beteiligt sind. Die Richtlinie kann ihre Weitergabe an andere Mitarbeiter von Mitgliedern der Gemeinschaft beschränken.

Die Richtlinie für den Informationsaustausch sollte die innerhalb der Gemeinschaft geltenden Regeln für die Kennzeichnung und Weitergabe von Informationen festlegen.

5.1.2 Überprüfung der Informationssicherheitsrichtlinien

ISO/IEC 27002:2013, Maßnahme 5.1.2, wird wie folgt erweitert:

Anleitung zur Umsetzung

Die Überprüfung sollte Informationen über wesentliche Änderungen bezüglich der Mitgliedschaft in der informationsaustauschenden Gemeinschaft enthalten.

6 Organisation der Informationssicherheit

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

7 Personalsicherheit

7.1 Vor der Beschäftigung

7.1.1 Sicherheitsüberprüfung

ISO/IEC 27002:2013, Maßnahme 7.1.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Es ist unwahrscheinlich, dass die Screening-Regeln für alle Mitglieder einer informationsaustauschenden Gemeinschaft einheitlich sind. Die Gemeinschaften sollten erwägen, ein Mindestniveau für Verifizierungsprüfungen festzulegen, die auf alle Mitarbeiter oder Auftragnehmer von Mitgliedern angewendet werden müssen, die Zugang zu in der Gemeinschaft geteilten Informationen erhalten.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

7.2 Während der Beschäftigung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

7.3 Beendigung und Änderung der Beschäftigung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

8.1.1 Inventarisierung der Werte

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.1.2 Zuständigkeit für Werte

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.1.3 Zulässiger Gebrauch von Werten

ISO/IEC 27002:2013, Maßnahme 8.1.3, wird wie folgt erweitert:

Anleitung zur Umsetzung

Informationen, die von anderen Mitgliedern einer informationsaustauschenden Gemeinschaft zur Verfügung gestellt werden, stellen einen Wert dar und sollten in Übereinstimmung mit den von der informationsaustauschenden Gemeinschaft oder vom Absender festgelegten Regeln geschützt, verwendet und weitergegeben werden.

8.1.4 Rückgabe von Werten

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.2 Informationsklassifizierung

8.2.1 Klassifizierung von Informationen

ISO/IEC 27002:2013, Maßnahme 8.2.1, wird wie folgt angepasst:

Maßnahme

Informationen sollten anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Glaubwürdigkeit, ihrer Priorität, ihrer Kritikalität und ihrer Sensibilität gegenüber unbefugter Offenlegung oder Veränderung klassifiziert werden.

Anleitung zur Umsetzung

Neben den in ISO/IEC 27002:2013 festgelegten Kriterien sollten Informationen im Hinblick auf ihre Glaubwürdigkeit und Priorität klassifiziert werden. Die Glaubwürdigkeit sollte anhand der Reputation der Quelle, des technischen Inhalts und der Qualität der Beschreibung beurteilt werden. Die Priorität sollte angeben, dass dringende oder sofortige Maßnahmen, wie eine erneute Weitergabe, erforderlich sind.

Ebenso kann die Sensibilität von vielen Aspekten der Informationen abhängen, die über die Notwendigkeit der Wahrung ihrer Vertraulichkeit hinausgehen, z. B. die Auswirkungen der Offenlegung oder das Potenzial, die Anonymität ihrer Quelle zu gefährden.

Klassifizierungskennzeichnungen, die von anderen Mitgliedern einer informationsaustauschenden Gemeinschaft vergeben wurden, sollten mit Bedacht interpretiert werden.

BEISPIEL Ein bekannter E-Mail-Client zeigt die Meldung „Bitte vertraulich behandeln“ bei der Anzeige von E-Mails an, bei denen das Kopffeld für die Vertraulichkeit auf „Firma (vertraulich)“ gesetzt wurde (RFC 4021 [1]). Es ist in diesem Fall nicht klar, ob der Absender „Firma (vertraulich)“ festlegen wollte (und die Nachricht versehentlich gesendet hat) oder ob der Absender „Vertraulich für Sie, den Empfänger“ festlegen wollte.

8.2.2 Kennzeichnung von Informationen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.2.3 Handhabung von Werten

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.3 Handhabung von Datenträgern

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

8.4 Schutz des Informationsaustauschs

Folgendes ist ein zusätzliches Maßnahmenziel zu ISO/IEC 27002:2013, Abschnitt 8, „Verwaltung der Werte“:

Ziel: Angemessener Schutz des Informationsaustauschs innerhalb einer informationsaustauschenden Gemeinschaft wird sichergestellt.

Informationen, die zwischen Mitgliedern einer informationsaustauschenden Gemeinschaft ausgetauscht werden, sollten auf einheitliche Weise geschützt werden, auch wenn die Mitglieder unabhängige Einheiten oder Teile von Einheiten sind, die ihre eigenen Informationen möglicherweise anders kennzeichnen, weitergeben und schützen.

Wenn Anonymität angefragt wird, sollten alle Informationen, die Rückschlüsse auf die Quelle des Informationsaustauschs zulassen, entfernt werden. Ebenso sollte es möglich sein, geteilte Informationen zu erhalten, ohne die Identität des Empfängers preiszugeben.

Die Veröffentlichung von geteilten Informationen außerhalb der Gemeinschaft sollte kontrolliert werden.

8.4.1 Weitergabe von Informationen

Maßnahme

Die Weitergabe von Informationen innerhalb des empfangenden Mitglieds sollte, basierend auf von der Gemeinschaft definierten Weitergabekennzeichnungen, begrenzt werden.

Anleitung zur Umsetzung

Informationen, denen keine Weitergabekennzeichnungen zugewiesen sind, sollten von der informationsaustauschenden Gemeinschaft definierte Standardrechte zur Weitergabe zugewiesen werden. Im Zweifelsfall oder wenn es keine allgemein akzeptierte Vereinbarung über die Weitergabe von Informationen gibt, sollten Informationen konservativ behandelt werden. Wenn möglich, sollte der Empfänger den Absender auffordern, die Informationen mit einer ausdrücklichen Weitergabekennzeichnung erneut zu senden.

Weitergabebeschränkungen können Verwendungsbeschränkungen beinhalten, wie z. B. Einschränkungen hinsichtlich des elektronischen Kopierens und Einfügens, das Verhindern von Screenshots oder das Verhindern von Druck und Export.

Weitere Informationen

Verschiedene Attribute oder Komponenten von geteilten Informationen können unterschiedlichen Sensibilitäten zugehörig sein. Insbesondere kann die Kenntnis des Vorhandenseins einer Nachricht oder anderer geteilter Informationen eine andere Sensibilität aufweisen, als deren Inhalt.

Häufig wird eine Funktion zur Verwaltung von Informationsrechten verwendet, um Einschränkungen in der Nutzung durchzusetzen. Wenn dies der Fall ist, ist eine klare Richtlinie oder ein klares Modell für Benutzerberechtigungen erforderlich, damit die Benutzer verstehen, was ihr System ihnen erlaubt und woran sie gehindert werden.

8.4.2 Haftungsausschluss für Informationen

Maßnahme

Jeder Informationsaustausch sollte mit einem Haftungsausschluss beginnen, in dem alle besonderen Anforderungen aufgeführt sind, die von den Empfängern zusätzlich zu den normalen Informationskennzeichnungen erfüllt werden müssen.

Anleitung zur Umsetzung

Ein Empfänger sollte den Absender um Klärung bitten, wenn der Haftungsausschluss nicht vollständig verstanden wurde oder nicht umgesetzt werden kann.

8.4.3 Glaubwürdigkeit von Informationen

Maßnahme

Bei jedem Informationsaustausch sollte das Maß an Vertrauen des Absenders in die Glaubwürdigkeit und Genauigkeit der gesendeten Informationen angegeben werden.

Anleitung zur Umsetzung

Aufgrund der Dringlichkeit, der möglichen Folgen und der technischen Einschränkungen ist es gegebenenfalls nicht möglich, alle Informationen vor der Übermittlung zu validieren. Wenn Beschränkungen bestehen, sollten diese als Teil der Nachricht angegeben werden.

Die Angabe von Vorbehalten gegen die Glaubwürdigkeit von Informationen ist besonders wichtig, wenn die Quelle anonym oder unbekannt ist. Es ist auch wichtig anzugeben, wenn der Absender die übermittelten Informationen direkt validieren konnte und für ihre Authentizität bürgen kann.

8.4.4 Verringerung der Sensibilität von Informationen

Maßnahme

Der Absender eines Informationsaustauschs sollte angeben, ob sich die Sensibilität der bereitgestellten Informationen nach einem externen Ereignis oder im Laufe der Zeit verringert.

Anleitung zur Umsetzung

Selbst wenn sich die Sensibilität der bereitgestellten Informationen mit der Zeit verringert, müssen sie möglicherweise weiterhin geschützt werden. Klassifizierungsrichtlinien (siehe 8.2.1) müssen möglicherweise Vorgaben zur Reduzierung der Sensibilität enthalten.

8.4.5 Schutz von anonymen Quellen

Maßnahme

Ein Mitglied einer Gemeinschaft sollte alle Informationen zur Identifizierung der Quelle in jeder gesendeten oder empfangenen Kommunikation entfernen, wenn Anonymität gefordert wird.

Anleitung zur Umsetzung

Der Absender der Informationen ist dafür verantwortlich, die Zustimmung der Quelle einzuholen (falls abweichend), bevor er die Informationen an andere Mitglieder der informationsaustauschenden Gemeinschaft weitergibt. Der Absender sollte die Quelle auch fragen, ob sie als der ursprüngliche Bereitsteller der Informationen identifiziert werden kann.

Es ist wichtig, dass beim Verfahren zum Schützen der Quelle sowohl der Nachrichteninhalt als auch die Nachrichtenherkunft betrachtet wird, da anhand einer Analyse des Inhalts die Identität der Quelle gegebenenfalls aufgedeckt werden kann. Wenn möglich, sollte der Absender der Nachricht die Quelle bitten, die anonymisierten Informationen und die Liste der vorgesehenen Empfänger zu überprüfen, bevor sie weitergegeben werden.

BEISPIEL Eine Nachricht wie „unsere Geldautomaten wurden heute durch einen neuen Virus deaktiviert, der nicht von unserer Firewall, sondern von unserem Richtlinienserver erkannt wurde“ könnte die Quelle aufdecken, wenn an dem betreffenden Tag nur eine Bank von einer öffentlichen Dienstunterbrechung betroffen wäre.

Es gibt technische Mechanismen, die genutzt werden können, um Authentizität sicherzustellen, ohne die Anonymität zu beeinträchtigen. So könnten beispielsweise gemeinsame kryptographische Geheimnisse verwendet werden, um zu bestätigen, dass eine Kommunikation von einem Mitglied der Gemeinschaft stammt, ohne die tatsächliche Identität des Absenders preiszugeben.

8.4.6 Schutz von anonymen Empfängern

Maßnahme

Mit Zustimmung des Absenders sollten die Mitglieder einer Gemeinschaft in der Lage sein, Mitteilungen zu empfangen, ohne ihre eigene Identität preiszugeben.

Anleitung zur Umsetzung

Der anonyme Empfang kann sowohl mit technischen Mitteln (z. B. Kryptographie) als auch mit verfahrenstechnischen Mitteln (z. B. Umleitung über eine unterstützende Stelle) realisiert werden. Es muss darauf geachtet werden sicherzustellen, dass die Anonymität nicht gegen gesetzliche Beschränkungen verstößt oder das allgemeine Vertrauen innerhalb der Gemeinschaft beeinträchtigt.

Weitere Informationen

Der anonyme Empfang ist oft erforderlich, um eine effektive sektorübergreifende Kommunikation sicherzustellen, da die Sektorgemeinschaften ihre Mitgliedschaftsdaten geheim halten möchten.

8.4.7 Berechtigung zur weiteren Weitergabe

Maßnahme

Sofern Informationen nicht für eine für weiter gefasste Veröffentlichung gekennzeichnet sind, sollten sie nicht ohne formelle Genehmigung des Absenders außerhalb der informationsaustauschenden Gemeinschaft weitergegeben werden.

Anleitung zur Umsetzung

Jeder Empfänger sollte dafür verantwortlich sein, alle erforderlichen Genehmigungen für eine weiter gefasste Veröffentlichung vom Absender einzuholen, bevor er sie weitergibt.

In der sektorübergreifenden Kommunikation kann der Absender nicht wissen, welche Organisationen die Informationen erhalten. In einem solchen Fall muss eine allgemeine oder spezifische Sektorfreigabe erteilt werden.

Weitere Informationen

Das Ampelprotokoll (siehe Anhang C) wird häufig verwendet, um anzugeben, inwiefern Informationen ohne zusätzliche Genehmigung weitergegeben werden können.

9 Zugangssteuerung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

10 Kryptographie

10.1 Kryptographische Maßnahmen

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

ISO/IEC 27002:2013, Maßnahme 10.1.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Kryptographische Techniken können auch zur Umsetzung der Weitergaberegeln für den Informationsaustausch eingesetzt werden, z. B. durch die Verwaltung von Informationsberechtigungen.

10.1.2 Schlüsselverwaltung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

11 Physische und umgebungsbezogene Sicherheit

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12 Betriebssicherheit

12.1 Betriebsabläufe und -verantwortlichkeiten

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.2 Schutz vor Schadsoftware

12.2.1 Maßnahmen gegen Schadsoftware

ISO/IEC 27002:2013, Maßnahme 12.2.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Informationen, die von anderen Mitgliedern einer informationsaustauschenden Gemeinschaft empfangen wurden, sollten auf das Vorhandensein von Schadsoftware überprüft werden, unabhängig davon, ob der Kommunikationsdienst zwischen den Mitgliedern der Gemeinschaft eine Nachrichtenüberprüfung umfasst oder nicht.

12.3 Datensicherung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.4 Protokollierung und Überwachung

12.4.1 Ereignisprotokollierung

ISO/IEC 27002:2013, Maßnahme 12.4.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Wenn es die informationsaustauschende Gemeinschaft erfordert, sollten die Mitglieder die interne Weitergabe von geteilten Informationen protokollieren.

12.4.2 Schutz der Protokollinformation

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.4.3 Administratoren- und Bedienerprotokolle

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.4.4 Uhrensynchronisation

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.5 Steuerung von Software im Betrieb

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.6 Handhabung technischer Schwachstellen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.7 Audits von Informationssystemen

12.7.1 Maßnahmen für Audits von Informationssystemen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

12.7.2 Auditberechtigungen in der Gemeinschaft

Folgendes ist eine zusätzliche Maßnahme zu ISO/IEC 27002:2013, 12.7, „Audit von Informationssystemen“:

Maßnahme

Jede informationsaustauschende Gemeinschaft sollte die Berechtigungen der Mitglieder zum Auditieren der Systeme anderer Mitglieder und vertrauenswürdiger Dienstleister festlegen.

Anleitung zur Umsetzung

Die Berechtigung zum Auditieren von Mitgliedssystemen könnte auf einen vertrauenswürdigen Dritten, wie eine vertrauenswürdige Einheit zur Informationsverbreitung (TICE) oder eine Warn-, Hinweis- und Meldestelle (WARP), beschränkt werden.

13 Kommunikationssicherheit

13.1 Netzwerksicherheitsmanagement

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

13.2 Informationsübertragung

13.2.1 Richtlinien und Verfahren für die Informationsübertragung

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

13.2.2 Vereinbarungen zur Informationsübertragung

ISO/IEC 27002:2013, Maßnahme 13.2.2, wird wie folgt erweitert:

Anleitung zur Umsetzung

Alle informationsaustauschenden Gemeinschaften sollten Vereinbarungen zur Informationsübertragung festlegen und den Mitgliedern nur dann den Beitritt zur Gemeinschaft gestatten, wenn derartige Vereinbarungen unterzeichnet und akzeptiert werden.

13.2.3 Elektronische Nachrichtenübermittlung

ISO/IEC 27002:2013, Maßnahme 13.2.3, wird wie folgt erweitert:

Anleitung zur Umsetzung

Alle informationsaustauschenden Gemeinschaften sollten Regeln für den Schutz von Informationen während der Übertragung festlegen und den Mitgliedern nur dann den Beitritt zur Gemeinschaft gestatten, wenn derartige Regeln von dem Mitgliedschaftskandidaten akzeptiert und umgesetzt werden. Jede unterstützende Stelle sollte derartige Regeln intern umsetzen.

Informationsaustauschende Gemeinschaften sollten die Einführung alternativer Mechanismen für den Informationsaustausch in Betracht ziehen, die nicht auf einem elektronischen Nachrichtenaustausch basieren, und es sollte Mitgliedern ermöglicht werden festzulegen, dass bestimmte Nachrichten über diese alternativen Mechanismen weitergegeben werden.

13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

15 Lieferantenbeziehungen

15.1 Informationssicherheit in Lieferantenbeziehungen

15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

ISO/IEC 27002:2013, Maßnahme 15.1.2, wird wie folgt erweitert:

Anleitung zur Umsetzung

Alle Mitglieder einer Gemeinschaft sollten über die Identität aller an der Erbringung von Dienstleistungen für die Gemeinschaft beteiligten Dritten informiert werden, falls Einwände gegen die Beteiligung bestimmter Parteien an der Verarbeitung der von ihnen bereitgestellten Informationen bestehen.

Die Vereinbarungen mit Lieferanten im Zusammenhang mit der Erbringung von Dienstleistungen für die Gemeinschaft sollten die regelmäßige Durchführung von Sicherheitsüberprüfungen und Audits der Dienstleistungen vorsehen.

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

15.2 Steuerung der Dienstleistungserbringung von Lieferanten

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16 Handhabung von Informationssicherheitsvorfällen

16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen

16.1.1 Verantwortlichkeiten und Verfahren

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16.1.2 Meldung von Informationssicherheitsereignissen

ISO/IEC 27002:2013, Maßnahme 16.1.2, wird wie folgt erweitert:

Anleitung zur Umsetzung

Die Mitglieder einer informationsaustauschenden Gemeinschaft sollten prüfen, ob erkannte Ereignisse an andere Mitglieder der Gemeinschaft gemeldet werden sollten. Die Gemeinschaft sollte Leitlinien zu den Arten von Vorfällen, die für andere Mitglieder von Interesse sein werden, vereinbaren und veröffentlichen. Mitglieder sollten anhand ihres Urteilsvermögens sicherstellen, dass nur Ereignisse gemeldet werden, die für andere Mitglieder potenziell von Interesse sind.

Es besteht eine starke Tendenz, dass Vorfälle vertraulich behandelt werden und ein Mitglied der Gemeinschaft keine Informationen zu Vorfällen preisgibt, um die Reputation des Absenders zu schützen. Die Weitergabe von Informationen über Vorfälle an andere wird jedoch die künftige Zusammenarbeit und Koordinierung bei der Vermeidung von Vorfällen fördern, eine sofortige und schnelle Reaktion auf Vorfälle ermöglichen und die allgemeine Sicherheit innerhalb der Gemeinschaft verbessern. Ereignisse und Vorfälle können gemeldet werden, ohne zwangsläufig all ihre Auswirkungen offenzulegen.

Ebenso sollten die Mitglieder alle gemeldeten Ereignisse unverzüglich untersuchen, um festzustellen, ob sie auch Auswirkungen auf ihren eigenen Betrieb haben. So könnte beispielsweise nach einer routinemäßigen Ankündigung von geplanten Wartungsarbeiten eines Mitglieds, das einen gemeinsam genutzten Dienst bereitstellt, erforderlich sein, dass andere Mitglieder die Zuverlässigkeit alternativer Anbieter überprüfen, bevor die Wartungsaktivität beginnt.

16.1.3 Meldung von Schwächen in der Informationssicherheit

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

ISO/IEC 27002:2013, Maßnahme 16.1.6, wird wie folgt erweitert:

Anleitung zur Umsetzung

Es sollten Untersuchungen auf der Grundlage von Informationen durchgeführt werden, die von einer informationsaustauschenden Gemeinschaft weitergegeben werden, um das Risiko ähnlicher Vorfälle zu verringern und ein besseres Verständnis der Risiken für die Gemeinschaft und alle damit verbundenen wichtigen Informationsinfrastrukturen zu erlangen. Solche Untersuchungen könnten von den betroffenen Mitgliedern der Gemeinschaft oder von einer unterstützenden Stelle durchgeführt werden, sofern diese vorhanden ist.

Nach gemeldeten Vorfällen sollten die Mitglieder der informationsaustauschenden Gemeinschaft Überprüfungen durchführen, um Pläne für Reaktionen auf Sicherheitsvorfälle, die zugehörigen Verfahren und das Geschäftsrisikoprofil zu aktualisieren, auch wenn das Mitglied von dem jeweiligen Vorfall nicht betroffen war. Jedes Mitglied sollte sicherstellen, dass gemeldete Reaktionen auf Vorfälle beurteilt und alle Erkenntnisse oder möglichen Verbesserungen der eigenen Prozesse des Mitglieds bestimmt und umgesetzt werden, um die eigenen Reaktionsprozesse fortlaufend zu verbessern.

16.1.7 Sammeln von Beweismaterial

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

16.1.8 Frühwarnsystem

Folgendes ist eine zusätzliche Maßnahme zu ISO/IEC 27002:2013, 16.1, „Handhabung von Informationssicherheitsvorfällen und Verbesserungen“:

Maßnahme

Innerhalb der informationsaustauschenden Gemeinschaft sollte ein Frühwarnsystem eingerichtet werden, um priorisierte Informationen effektiv zu kommunizieren, sobald sie verfügbar sind.

Anleitung zur Umsetzung

Priorisierte Informationen sind Informationen, die es anderen Mitgliedern der Gemeinschaft ermöglichen können, ähnliche unerwünschte Ereignisse zu vermeiden oder zu minimieren. Es ist wichtig, dass solche Informationen mit hoher Dringlichkeit weitergegeben werden, auch wenn sie nicht vollständig analysiert oder bestätigt worden sind.

17 Informationssicherheitsaspekte beim Business Continuity Management

17.1 Aufrechterhalten der Informationssicherheit

17.1.1 Planung der Aufrechterhaltung der Informationssicherheit

ISO/IEC 27002:2013, Maßnahme 17.1.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Von Mitgliedern einer informationsaustauschenden Gemeinschaft entwickelte Pläne für die Aufrechterhaltung des Geschäfts und die Notfallwiederherstellung sollten der Notwendigkeit Rechnung tragen, sensible Informationen mit anderen Mitgliedern im Rahmen des Wiederherstellungsprozesses auf sichere Weise auszutauschen.

17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

17.2 Redundanzen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

18 Compliance

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

ISO/IEC 27002:2013, Maßnahme 18.1.1, wird wie folgt erweitert:

Anleitung zur Umsetzung

Die informationsaustauschende Gemeinschaft sollte alle relevanten Vereinbarungen, Gesetze und Vorschriften in Bezug auf den Informationsaustausch, wie z. B. Kartellgesetze oder -vorschriften, einhalten. Dadurch könnte verhindert werden, dass bestimmte Organisationen der Gemeinschaft beitreten, oder deren Repräsentation könnte eingeschränkt werden.

18.1.2 Geistige Eigentumsrechte

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

18.1.3 Schutz von Aufzeichnungen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

18.1.4 Privatsphäre und Schutz von personenbezogenen Informationen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

18.1.5 Regelungen bezüglich kryptographischer Maßnahmen

Keine zusätzlichen Informationen, die für die sektor- und organisationsübergreifende Kommunikation spezifisch sind.

18.1.6 Haftung gegenüber der informationsaustauschenden Gemeinschaft

Folgendes ist eine zusätzliche Maßnahme zu ISO/IEC 27002:2013, 18.1, „Einhaltung von rechtlichen und vertraglichen Anforderungen“:

Maßnahme

Haftungsfragen und Abhilfemaßnahmen sollten von allen Mitgliedern einer informationsaustauschenden Gemeinschaft geklärt, verstanden und genehmigt werden, um Situationen gerecht zu werden, in denen Informationen absichtlich oder unabsichtlich weitergegeben werden.

Anleitung zur Umsetzung

Die Abhilfemaßnahmen sollten mindestens eine Benachrichtigung an den Absender über jede unbefugte Weitergabe beinhalten, mit ausreichenden Einzelheiten, um die offenbarten Informationen zu identifizieren.

Wenn möglich, sollte die Benachrichtigung an die Quelle zurückgegeben werden, auch wenn die Informationen bereinigt wurden und die Herkunft nicht offenbart wurde. Dies könnte durch die Vermittlung eines vertrauenswürdigen Dritten, wie beispielsweise einer vertrauenswürdigen Einheit zur Informationsverbreitung (TICE), erreicht werden.