

DIN EN 16495

ICS 03.220.50; 35.240.60

Einsprüche bis 2013-01-05

Entwurf**Flugverkehrsmanagement –
Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt;
Deutsche und Englische Fassung prEN 16495:2012**

Air Traffic Management –
Information security for organisations supporting civil aviation operations;
German and English version prEN 16495:2012

Gestion du trafic aérien –
Sécurité de l'information;
Version allemande et anglaise prEN 16495:2012

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2012-11-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an nl@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de, sofern dort wiedergegeben;
- oder in Papierform an den Normenausschuss Luft- und Raumfahrt (NL) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

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

Gesamtumfang 125 Seiten

Normenausschuss Luft- und Raumfahrt (NL) im DIN

Nationales Vorwort

Dieses Dokument (prEN 16495:2012) wurde im Technischen Komitee CEN/TC 377 „Luftverkehrsmanagement“ (Sekretariat: DIN, Deutschland) erarbeitet.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-05-02 AA „Flugverkehrsmanagement (ATM) (SpA CEN/TC 377)“ im DIN Normenausschuss Luft- und Raumfahrt.

Entsprechend Beschluss 57/9 des Technischen Ausschusses des Beirats des Normenausschusses Luft- und Raumfahrt (NL) im DIN Deutsches Institut für Normung e. V. sind die europäischen Luft- und Raumfahrt-Normungsergebnisse zweisprachig, in Deutsch und Englisch, in das Deutsche Normenwerk zu überführen. Aus diesem Grund wurde der Deutschen Fassung dieses Dokuments die Englische Fassung hinzugefügt.

Flugverkehrsmanagement — Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

Gestion du trafic aérien — Sécurité de l'information

Air Traffic Management — Information security for organisations supporting civil aviation operations

ICS:

Deskriptoren

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

STD Version 2.4e - RC2

Inhalt

Seite

Vorwort	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Informationssicherheitsmanagement in der Luftfahrt	5
4.1 Aufbau dieser Europäischen Norm	5
4.2 Informationssicherheitsmanagementsysteme in der Luftfahrt	6
4.3 Analyse und Bewertung von Informationssicherheitsrisiken	6
4.4 Auswahl von Maßnahmen	10
4.5 Anwendbarkeitserklärung	10
4.6 Vertrauensstufen	11
4.7 Messung und Auditierung der Sicherheit	12
5 Sicherheitsleitlinie	13
5.1 Informationssicherheitsleitlinie	13
6 Organisation der Informationssicherheit	13
6.1 Interne Organisation	13
6.2 Externe Parteien	15
7 Management organisationseigener Werte (Assets)	15
7.1 Verantwortung für organisationseigene Werte (Assets)	15
7.2 Klassifizierung von Informationen	16
8 Sicherheit personeller Ressourcen	17
8.1 Vor der Einstellung	17
8.2 Während der Anstellung	17
8.3 Beendigung oder Wechsel der Anstellung	18
9 Physische und umgebungsbezogene Sicherheit	18
9.1 Sicherheitsbereiche	18
9.2 Sicherheit von Ausrüstungen	19
10 Kommunikations- und Betriebsmanagement	20
10.1 Den Betrieb betreffende Verfahren und Verantwortlichkeiten	20
10.2 Management der Erbringung von Dienstleistungen durch Dritte	20
10.3 Systemplanung und Abnahme	21
10.4 Schutz vor Schadsoftware und mobilen Programmcodes	21
10.5 Backup	21
10.6 Management der Netzsicherheit	22
10.7 Umgang mit Medien	22
10.8 Austausch von Informationen	22
10.9 Dienstleistungen im Rahmen des elektronischen Geschäftsverkehrs	23
10.10 Überwachung	23
11 Zugangskontrolle	24
11.1 Geschäftsanforderungen an die Zugangskontrolle	24
11.2 Benutzerverwaltung	24
11.3 Benutzerverantwortung	26
11.4 Zugangskontrolle für Netze	26
11.5 Steuerung des Zugriffs auf Betriebssysteme	27
11.6 Zugangskontrolle für Anwendungen und Informationen	28
11.7 Mobile Computing und Telearbeit	29
12 Beschaffung, Entwicklung und Aufrechterhaltung von Informationssystemen	29

12.1	Sicherheitsanforderungen an Informationssysteme	29
12.2	Ordnungsgemäße Verarbeitung in Anwendungen	30
12.3	Kryptografische Maßnahmen	31
12.4	Sicherheit von Systemdateien	32
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen	32
12.6	Verwaltung technischer Schwachstellen	33
13	Behandlung von Informationssicherheitsvorfällen	34
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen	34
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen	35
14	Betriebskontinuitätsmanagement	36
14.1	Informationssicherheitsaspekte hinsichtlich des Betriebskontinuitätsmanagements	36
15	Übereinstimmung	38
15.1	Übereinstimmung mit gesetzlichen Anforderungen	38
15.2	Übereinstimmung mit Sicherheitsrichtlinien und -normen sowie technische Übereinstimmung	38
15.3	Betrachtungen bezüglich Audits von Informationssystemen	39
Anhang A	(informativ) Beispiele für die Umsetzung	40
A.1	Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB)	41
A.2	Organisationsübergreifende Verbindungen/externe Verbindungen (LoT-A-NET)	42
A.3	Zertifikate/Public-Key-Infrastruktur (LoT-A-PKI)	47
A.4	Identitätsmanagement (LoT-A-IDM)	48
Anhang B	(informativ) Vertrauensstufe – Beispiel für die Umsetzung	50
Literaturhinweise		59

Vorwort

Dieses Dokument (prEN 16495:2012) wurde vom Technischen Komitee CEN/TC 377 „Luftverkehrsmanagement“ erarbeitet, dessen Sekretariat vom DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

1 Anwendungsbereich

Diese Europäische Norm legt Leitlinien und allgemeine Grundsätze für die Umsetzung eines Informationssicherheits-Managementsystems in Organisationen im Bereich der Zivilluftfahrt fest.

Nicht in den Anwendungsbereich fallen Handlungen der Organisationen, die sich nicht auf die Sicherheit von Tätigkeiten im Bereich der Zivilluftfahrt auswirken, wie z. B. Management von Einzelhandelsgeschäften am Flughafen und Dienstleistungsunternehmen sowie Management von Unternehmensimmobilien (en: corporate real estate management).

Für die Zwecke dieser Europäischen Norm wird Flugverkehrsmanagement als funktioneller Begriff betrachtet, der die Verantwortlichkeiten aller an der Wertschöpfungskette im Luftverkehr Beteiligten abdeckt. Das betrifft Luftraumnutzer, Flughäfen und Flugsicherungsorganisationen, ist jedoch nicht allein darauf beschränkt.

Grundlage für alle Anforderungen in dieser Europäischen Norm sind das Vertrauen und die Zusammenarbeit zwischen den Parteien, die am Flugverkehrsmanagement beteiligt sind.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000:2009 und die folgenden Begriffe.

3.1

Flugverkehrsmanagement

Zusammenfassung der bordseitigen und bodenseitigen Funktionen (Flugverkehrsdienste, Luftraummanagement und Verkehrsflussregelung), die für die sichere und effiziente Bewegung von Luftfahrzeugen in allen Betriebsphasen erforderlich sind

3.2

Vertrauen

Situation, in der eine Partei bereit dazu ist, sich auf die Handlungen einer anderen Partei zu verlassen

Anmerkung 1 zum Begriff: Vertrauen ist mehr als das, was mittels Versicherung erreicht werden kann. Versicherung stellt jedoch ein unterstützendes Instrument für die Vertrauensbildung dar.

4 Informationssicherheitsmanagement in der Luftfahrt

4.1 Aufbau dieser Europäischen Norm

Der Aufbau dieser Europäischen Norm ist an ISO/IEC 27002 angepasst. In allen Fällen, in denen die Maßnahmen nach ISO/IEC 27002 ohne Änderung oder Ergänzung angewendet werden können, wird lediglich auf ISO/IEC 27002 verwiesen.

In allen Fällen, in denen die Umsetzung von Maßnahmen nach ISO/IEC 27002 eine für die Luftfahrt spezielle Ergänzung erfordert, wurde das direkt in den betreffenden Abschnitt aufgenommen.

Umsetzungsbeispiele für besondere Anwendungsbereiche sind im informativen Anhang A beschrieben. Das betrifft folgende Bereiche:

- Sicherheit von Informationen in Web-Anwendungen und Web-Diensten;
- Verbindungen zwischen mehreren Organisationen/externe Verbindungen;
- Zertifikate/ Infrastruktur für öffentliche Schlüssel (en: Public Key Infrastructure);
- Identitätsmanagement.

4.2 Informationssicherheitsmanagementsysteme in der Luftfahrt

Diese Europäische Norm ist eine Leitlinie für die Umsetzung und Steuerung eines Informationssicherheitsmanagementsystems in Luftfahrtorganisationen. Sie beruht auf der Internationalen Norm ISO/IEC 27002 (Leitfaden für das Informationssicherheitsmanagement). Luftfahrtorganisationen sollten zusätzlich zu den Zielen und Maßnahmen nach ISO/IEC 27002 auch die in dieser Europäischen Norm aufgeführten Sicherheitsmaßnahmen beachten.

Das Informationssicherheitsmanagement hat in der Luftfahrt hohe Priorität, unabhängig von der jeweiligen Stellung der Organisation innerhalb der Dienstleistungskette. Ohne ein wirksames Informationssicherheitsmanagementsystem nehmen die Risiken in Verbindung mit der Vertraulichkeit, Verfügbarkeit und Integrität der zur Erbringung von Dienstleistungen erforderlichen Informationen/Daten in kritischem Maße zu.

Die Erbringung von Dienstleistungen in der Luftfahrt ist in hohem Maße von der Zusammenarbeit der einzelnen Beteiligten bestimmt. Das Informationssicherheitsmanagement einer Organisation hängt daher vom Informationssicherheitsmanagement derjenigen Organisationen ab, mit denen die betreffende Organisation zur Erbringung von Dienstleistungen zusammenarbeitet. Diese Europäische Norm konzentriert sich daher auf die Aspekte der Zusammenarbeit.

Diese Zusammenarbeit erfordert

- die gemeinsame Nutzung der Ergebnisse von Risikobeurteilungen in der gesamten Geschäftsprozesskette;
- die Übereinstimmung hinsichtlich des erforderlichen Maßes an Vertrauen;
- die Übereinstimmung hinsichtlich der erforderlichen Sicherheitskontrollen und ihrer Umsetzung.

4.3 Analyse und Bewertung von Informationssicherheitsrisiken

4.3.1 Internes Informationssicherheitsrisiko-Management

Um ihre eigene Sicherheitslage verstehen zu können, muss eine Organisation die Sicherheitslage ihrer Partner kennen.

Die Herstellung von Netzverbindungen und der Austausch von Daten beruht auf einer Vertrauensbewertung der beteiligten Parteien untereinander. Der Umfang, mit dem der Netzwerkverkehr und die Daten gesteuert und überprüft werden müssen, wird durch das Maß an Vertrauen bestimmt.

Zur Ermöglichung einer sicheren Verbindung nach außen und eines sicheren Datenaustausches muss die Organisation das Vertrauen bewerten, das sie in die Verbindung und die empfangenen Daten setzen kann und sie muss sich davon überzeugen, dass die Vertrauensbewertung validiert ist.

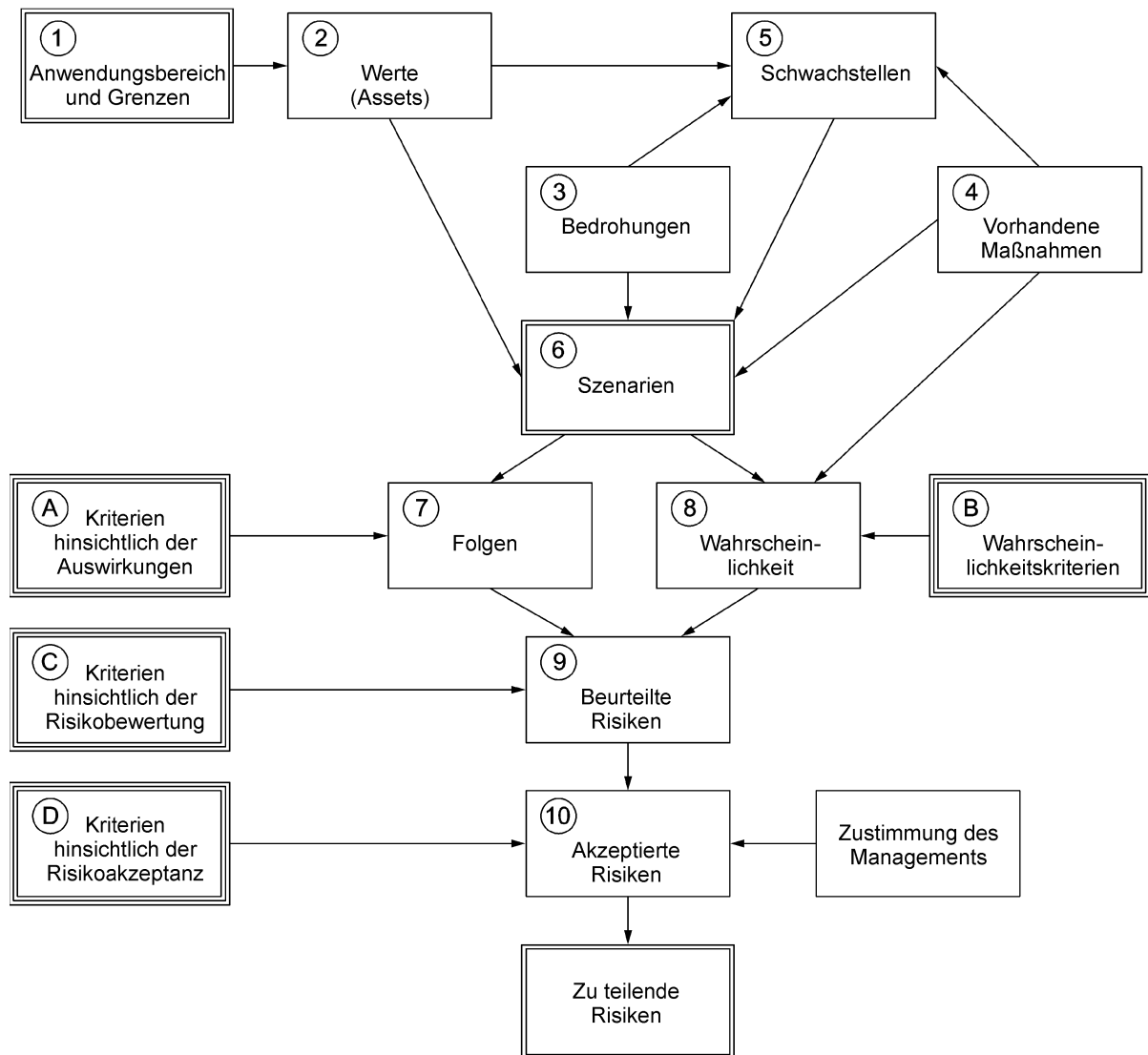
Es muss betont werden, dass das nicht bedeutet, dass die Organisation alles über die Sicherheit ihrer Partner wissen muss. Es werden lediglich genügend Informationen benötigt, um auf der Grundlage von Risikobewertungen das erforderliche Maß an Gewissheit zu erlangen.

Auf der Grundlage einer gemeinsamen Reihe von Parametern und Prozessen können generische Interkonnektivitätsfälle konstruiert und bewertet werden. Wenn diese Fälle auf konkrete Interkonnektivitätsfälle zutreffen, sind keine zusätzlichen Risikobewertungen notwendig. Ein Beispiel für einen generischen Interkonnektivitätsfall kann Anhang A entnommen werden.

Die Organisationen müssen diese Informationen im erforderlichen Maß mit ihren Partnern in der Zivilluffahrt gemeinsam nutzen. Diese Europäische Norm legt fest, welche Informationen gemeinsam genutzt werden müssen.

Der zugrunde liegende Prozess der Risikobewertung ist mit ISO/IEC 27005:2011 verträglich. Das gilt insbesondere für die nachstehend verwendete Terminologie.

ANMERKUNG In Abhängigkeit von der angewendeten Methodik dürfen die in den nachfolgenden Abschnitten beschriebenen Maßnahmen auch in einer anderen Reihenfolge durchgeführt werden.



Legende

Doppelt umrandete Kästchen enthalten die Informationen, die nach 4.3.3 gemeinsam zu nutzen sind.

Dreifach umrandete Kästchen enthalten die Kriterien, die als Teil des Risikomanagementprozesses der Organisation festzulegen sind. Sie werden dann als feststehende Eingaben für die einzelnen Risikobewertungen verwendet.

Bild 1

A. Kriterien hinsichtlich der Auswirkungen

Bezüglich des Ausmaßes von Schäden oder Kosten für die Organisation, die durch ein Informationssicherheitsereignis verursacht werden, sollte Kriterien hinsichtlich der Auswirkungen entwickelt und festgelegt werden.

B. Kriterien für die Beurteilung der Wahrscheinlichkeit

Es sollten Kriterien für die Beurteilung der Wahrscheinlichkeit entwickelt werden, die in ähnlicher Weise von beteiligten und beeinträchtigten Organisationen verstanden werden.

C. Kriterien hinsichtlich der Risikobewertung

Es sollten Risikobewertungskriterien zur Beurteilung des Informationssicherheitsrisikos der Organisation entwickelt werden, wobei Folgendes zu berücksichtigen ist:

- der strategische Wert des Geschäftsinformationsprozesses;
- die Kritikalität der betroffenen Informationswerte;
- gesetzliche und behördliche Anforderungen und vertragliche Verpflichtungen;
- betriebliche und geschäftliche Bedeutung von Verfügbarkeit, Vertraulichkeit und Integrität;
- Erwartungen und Wahrnehmungen der Beteiligten sowie negative Auswirkungen auf den Geschäftswert und das Ansehen der Organisation.

D. Kriterien hinsichtlich der Risikoakzeptanz

Hinsichtlich der Risikoakzeptanz sollten Kriterien entwickelt und festgelegt werden.

Der **Prozess der Risikobewertung** sollte folgende Schritte umfassen.

Schritt 1 – Anwendungsbereich und Grenzen:

Funktion: Sicherstellung, dass alle maßgeblichen Werte berücksichtigt werden und Bewertung von Risiken, die über die Grenzen der Organisation hinausgehen könnten. Darüber hinaus sollte die Organisation für alle Ausschlüsse aus dem Anwendungsbereich eine Begründung bereithalten.

Ergebnisse: Festlegung des Anwendungsbereiches und der Grenzen der Bewertung.

Schritt 2 – Werte:

Funktion: Identifizierung von allem, was für die Organisation von Wert ist und dessen Schutz daher erforderlich ist. Ein Wert (Asset) muss über eine individuelle Reihe von Merkmalen verfügen, die auf Bedrohungen und Schwachstellen bezogen werden können, um die Analyse in den folgenden Schritten zu ermöglichen.

Ergebnisse: Eine Auflistung von Werten, die risikobewertet werden müssen sowie eine Auflistung von Geschäftsprozessen, die sich auf die Werte und ihre Relevanz zusammen mit den entsprechenden Eigentümern der Werte beziehen.

Schritt 3 – Bedrohungen:

Funktion: Identifizierung von Bedrohungen, die über das Potential verfügen, Werte, wie z. B. Informationen, Prozesse und Systeme zu schädigen. Eine Bedrohung kann innerhalb oder außerhalb der Organisation entstehen.

Ergebnisse: Eine Auflistung von Bedrohungen mit Identifizierung der Art und Quelle der Bedrohung.

Schritt 4 – Vorhandene Maßnahmen

Funktion: Identifizierung vorhandener oder geplanter Maßnahmen, um zu erkennen, wie sich dadurch die Wahrscheinlichkeit von Bedrohungen sowie die Einfachheit der Ausnutzung von Schwachstellen oder die Auswirkung eines Ereignisses verringern würden.

Ergebnisse: Auflistung aller bereits durchgeführten und geplanten Maßnahmen, ihrer Umsetzung und des Anwendungsstatus.

Schritt 5 – Schwachstellen:

Funktion: Identifizierung von Merkmalen der Werte (Assets) sowie von Geschäftsprozessen, die für einen Angriff ausgenutzt werden können. Zum Zeitpunkt der Bewertung werden nicht alle Schwachstellen bekannt sein (insbesondere die technischen so genannten Zero-Day-Schwachstellen). Diese Möglichkeit muss mittels Sicherheitsmaßnahmen angesprochen werden, die eine schnelle Neubewertung des Risikos bei Entdeckung der Schwachstellen ermöglichen.

Ergebnisse: Auflistung von Schwachstellen bezüglich der Werte, Bedrohungen und Maßnahmen.

Schritt 6 – Szenarien:

Funktion: Identifizierung der Auswirkungen auf die Organisation, die durch ein Bedrohungsszenario verursacht werden könnten. Ein Bedrohungsszenario ist die Beschreibung einer Bedrohung, die eine bestimmte Schwachstelle oder Gruppe von Schwachstellen ausnutzt, um trotz vorhandener Kontrollmaßnahmen Werte anzugreifen.

Ergebnisse: Auflistung von Bedrohungsszenarien mit ihren jeweiligen Auswirkungen bezogen auf die Werte und Geschäftsprozesse der Organisation sowie weiterer betroffener Organisationen.

Schritt 7 – Folgen (Bewertung):

Funktion: Bewertung der Folgen jedes Szenarios, bezogen auf die Einschätzung des Wertes (Assets) und auf der Grundlage der Kriterien für die geschäftlichen Auswirkungen.

Ergebnisse: Auflistung der bewerteten Folgen eines Ereignisszenarios, angegeben hinsichtlich der Werte und Auswirkungskriterien.

Schritt 8 – Wahrscheinlichkeit:

Funktion: Bewertung der Wahrscheinlichkeit für das Auftreten eines jeden Szenarios.

Ergebnisse: Wahrscheinlichkeit von Bedrohungsszenarien (quantitativ und qualitativ).

Schritt 9 – Beurteiltes Risiko:

Funktion: Umwandeln von Szenarien in beurteilte Risiken auf der Grundlage der Folgen und der Wahrscheinlichkeit sowie der Risikobewertungskriterien, die während der Herstellung des Zusammenhangs festgelegt wurden. Die Summierung mehrerer kleiner oder mittlerer Risiken kann zu wesentlich größeren Gesamtrisiken führen und muss entsprechend behandelt werden.

Ergebnisse: Auflistung von Risiken, die entsprechend den Risikobewertungskriterien bezüglich der Bedrohungsszenarien, die zu diesen Risiken führen, klassifiziert werden.

Schritt 10 – Bewertetes Risiko:

Funktion: Bewertung der Auflistung klassifizierter Risiken hinsichtlich der Annehmbarkeit auf der Grundlage der zuvor festgelegten Risikoakzeptanzkriterien.

Ergebnisse: Auflistung bewerteter Risiken mit den zugehörigen Bedrohungsszenarien, die entsprechend den Risikoakzeptanzkriterien bevorzugt zu behandeln sind. Das schließt Informationen über die Folgen und die Wahrscheinlichkeit für jedes Risiko ein.

4.3.2 Probleme der Interoperabilität von Risikobewertungen

Die Interoperabilität von Risikobewertungen ist ein wichtiges Problem in einer Umgebung, die als „übergeordnetes System“ gekennzeichnet werden kann. In solch einer Umgebung sind Risikobewertungen, die (Teilbereiche von) diesen Systemen abdecken, vorhanden und es ist wichtig, die Übereinstimmungen zwischen den identifizierten Risiken und den Abschwächungsmaßnahmen, die in diesen Bewertungen vorgeschlagen werden, zu ermitteln. Dadurch wird eine schlüssige Sicherheitspolitik für das gesamte vielschichtige System ermöglicht.

Um die Interoperabilität von Risikobewertungen zu erreichen, wenn unterschiedliche methodische Vorgehensweisen bei der Risikobewertung angewendet werden,

- muss eine Verständigung hinsichtlich der Übereinstimmung zwischen den Themen/Begriffen/Benennungen, die in jede der zugrunde liegenden methodischen Vorgehensweisen für die Risikobewertung eingeführt wurden, erfolgen; und
- die Tiefe und Breite jeder Bewertung müssen verglichen und bewertet werden, um die vorausgesetzte Umgebung und die Entscheidungen hinsichtlich des Sicherheitsniveaus des vorliegenden Systems zu verstehen.

Terminologieprobleme können ebenso relevant sein, da es selbst bei gleichen zugrunde liegenden Verfahren vorkommen kann, dass Themen/Begriffe/Benennungen unterschiedlichen Bedeutungen zugeordnet sind.

4.3.3 Informationssicherheitsrisikomanagement für mehrere Organisationen

Um die Vergleichbarkeit über mehrere Organisationen hinweg sicherzustellen, müssen die Organisationen mindestens die Informationen zum Anwendungsbereich und den Grenzen, zu den Bedrohungsszenarien und den bewerteten Risiken gemeinsam nutzen.

Die gemeinsame Nutzung von Informationen sollte darauf beruhen, in dem erforderlichen Maße das Verfahren zu kennen, um mit geteilten Risiken umzugehen. Aufgrund der sensiblen Art der Auflistungen von bewerteten Risiken, werden diese Ergebnisse üblicherweise von jeder Organisation intern ermittelt und intern vertraulich behandelt.

Der Austausch der Informationen muss durch bindende Vertraulichkeitsvereinbarungen in geeigneter Form zwischen den betroffenen Organisationen unterstützt werden.

4.4 Auswahl von Maßnahmen

Maßnahmen sollten in Übereinstimmung mit den Ergebnissen der Informationssicherheitsrisikoanalyse ausgewählt und umgesetzt werden:

- Maßnahmen nach ISO/IEC 27002;
- Maßnahmen, die die in ISO/IEC 27002 angegebenen ergänzen. Diese Maßnahmen sind in dieser Europäischen Norm als für die luftverkehrsspezifische Umsetzungsvorgaben beschrieben.

4.5 Anwendbarkeitserklärung

Die Organisation sollte eine „Anwendbarkeitserklärung“ erstellen, aus der hervorgeht, welche Maßnahmen innerhalb des entsprechenden Anwendungsbereiches umgesetzt werden, und welche Maßnahmen als „nicht anwendbar“ betrachtet werden. Die „Anwendbarkeitserklärung“ sollte einem Partner sofern notwendig bekannt gegeben werden.

4.6 Vertrauensstufen

4.6.1 Einleitung

Wie bereits zuvor in 4.2 ausgeführt, ist die Erbringung von Dienstleistungen in der Luftfahrt von einem hohen Maß an Zusammenarbeit zwischen den beteiligten Organisationen geprägt. Die Gewährleistung der Sicherheit der Informationen und der informationsverarbeitenden Systeme einer einzelnen Organisation in einem gemeinsamen Geschäftsvorgang sowie der dahinter stehenden eigenen Geschäftsvorgänge haben ein hohes Maß an individuellen Vereinbarungen und Überprüfungen zur Folge.

Luftfahrtorganisationen, die in Partnerschaft arbeiten, sollten vereinbaren, dass in weiteren gemeinsamen Geschäftsabläufen (einschließlich denen mit dritten Parteien) Vertrauensstufen anerkannt werden, unterstützt durch sinnvolle Nachweise (aus der 1 : 1-Beziehung zweier Parteien oder über eine Verifizierung durch Dritte).

Die „Vertrauensstufe der Organisation“ (LoT-O) (en: Level of Trust of the organisation) bezieht sich auf die jeweilige Organisation. Die Einstufung bezieht sich dabei immer auf den Teil des gemeinsamen Prozesses, der von der jeweiligen Organisation erbracht wird. Insbesondere werden dabei mögliche Informationssicherheitsrisiken berücksichtigt, die für die jeweilige Partei durch Koppelung der Geschäftsprozesse entstehen können.

Zusätzlich zur Gesamtbewertung der Organisation kann eine Vertrauensstufe auch einer bestimmten Anwendung in einem Teilbereich wie in den Beispielen in Anhang A beschrieben zugeordnet werden.

4.6.2 Skala der Vertrauensstufen

Zur Einstufung der „Vertrauensstufe der Organisation“ wird eine sechsstufige Skala verwendet:

- vertrauenswürdig;
- begrenzt vertrauenswürdig 0;
- begrenzt vertrauenswürdig 1;
- begrenzt vertrauenswürdig 2;
- begrenzt vertrauenswürdig 3;
- nicht vertrauenswürdig.

Die allgemeinen Definitionen für die verschiedenen Stufen sollten wie folgt sein:

a) vertrauenswürdig:

Die Kategorie „vertrauenswürdig“ wird nur für organisationseigene Abteilungen, Tochterunternehmen oder Geschäftsprozesse angewendet, die vollständig den eigenen Sicherheitsanforderungen unterliegen. Drittpartei-Organisationen können nicht in die Kategorie „vertrauenswürdig“ eingestuft werden.

b) begrenzt vertrauenswürdig 0:

Die Kategorie „begrenzt vertrauenswürdig 0“ (LT0) bezeichnet Drittpartei-Organisationen oder unternehmens-eigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, jedoch folgende Anforderungen erfüllen:

Alle Maßnahmen dieser Europäischen Norm sind verbindlich umgesetzt. Die Übereinstimmung mit der Norm wurde von einem qualifizierten Informationssicherheits-Auditor bestätigt.

ANMERKUNG Das kann z. B. ein zertifizierter Informationssystem-Auditor (CISA), ein Auditleiter nach ISO/IEC 27001 oder ein gleichwertiger Sachkundiger sein.

c) **begrenzt vertrauenswürdig 1:**

Die Kategorie „begrenzt vertrauenswürdig 1“ (LT1) bezeichnet Drittpartei-Organisationen oder unternehmens-eigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein sehr hohes Gesamtniveau an Informationssicherheit erreichen. Das trifft auch auf Bereiche zu, in denen lediglich indirekte Risiken für die Partner Organisationen bestehen.

BEISPIEL 1 Kopplung von Netzwerken

Organisationen werden unter bestimmten Umständen den Zugriff von Partnerorganisationen mit LT1-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, ohne anwendungsspezifische Schutzmaßnahmen (z. B. Web Application Firewalls) und ohne weitere Authentisierung an der Netzwerkgrenze (z. B. an der Firewall) durchzusetzen.

Dieses Vorgehen ist nur dann angemessen, wenn der Partner über ein sehr hohes Sicherheitsniveau (LT1) verfügt und in diesem Zusammenhang alle maßgeblichen Informationssicherheitsmanagementsystem-Maßnahmen umgesetzt hat.

d) **begrenzt vertrauenswürdig 2:**

Die Kategorie „begrenzt vertrauenswürdig 2“ (LT2) bezeichnet Drittpartei-Organisationen oder unternehmens-eigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein hohes Gesamtniveau an Informationssicherheit erreichen.

BEISPIEL 2 Kopplung von Netzwerken

Organisationen werden unter bestimmten Umständen den Zugriff von Partnerorganisationen mit LT2-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, aber vor dem Verbindungsaufbau an der Netzwerkgrenze (z. B. an der Firewall) eine explizite Authentisierung fordern.

Dieses Vorgehen ist nur dann angemessen, wenn der Partner über ein hohes Sicherheitsniveau (LT2) verfügt und in diesem Zusammenhang alle wichtigen Informationssicherheitsmanagementsystem-Maßnahmen (z. B. Management von Sicherheitsvorfällen) umgesetzt hat.

e) **begrenzt vertrauenswürdig 3:**

Die Kategorie „begrenzt vertrauenswürdig 3“ (LT3) bezeichnet Drittpartei-Organisationen oder unternehmens-eigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein Basis-Niveau an Informationssicherheit erreichen.

BEISPIEL 3 Kopplung von Netzwerken

Organisationen werden unter bestimmten Umständen den Zugriff von Partnern mit LT3-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, aber vor dem Verbindungsaufbau an der Netzwerkgrenze (z. B. an der Firewall) sowohl eine explizite Authentisierung fordern als auch weitere Schutzmaßnahmen (z. B. Content-Filterung, Eingabe-Kontrolle, Rechteverwaltung usw.).

Dieses Vorgehen ist nur dann angemessen, wenn der Partner Basis-Sicherheitsmaßnahmen (z. B. Virenschutz, Backup/Restore usw.) sowie ein Sicherheitsmanagementsystem umgesetzt hat.

f) **nicht vertrauenswürdig:**

Diese Kategorie bezeichnet alle Organisationen, welche die Anforderungen der Kategorie „begrenzt vertrauenswürdig 3“ nicht erfüllen.

4.6.3 Klassifizierungskriterien

Die Einzelheiten der speziellen Maßnahmen, die für die unterschiedlichen Vertrauensstufen umzusetzen sind, sollten von den zusammenarbeitenden Organisationen festgelegt werden. Ein Beispiel für die Umsetzung von Vertrauensstufen für eine Organisation kann Anhang B entnommen werden.

4.7 Messung und Auditierung der Sicherheit

Die Messung der Wirksamkeit der umgesetzten Kontrollmaßnahmen sollte unter Berücksichtigung der Leitlinien nach ISO/IEC 27004 erfolgen.

Interne Auditierungsmaßnahmen sollten unter Berücksichtigung der zusätzlichen Hinweise in ISO/IEC 27007 durchgeführt werden.

5 Sicherheitsleitlinie

5.1 Informationssicherheitsleitlinie

Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit.

Das Management sollte eine klare Richtung der Grundsätze vorgeben und Unterstützung und Engagement für Informationssicherheit durch organisationsweite Veröffentlichung und Aufrechterhaltung einer Informationssicherheitsleitlinie unter Beweis stellen.

5.1.1 Dokument der Informationssicherheitsleitlinie

Die in ISO/IEC 27002:2005, 5.1.1, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Leitlinie zur Informationssicherheit sollte mit den vielfältigen Sicherheitsanforderungen in anderen Bereichen des Luftverkehrs (z. B. physische Absicherung von Sicherheitsbereichen) abgestimmt werden. Die Abgrenzungen und gegenseitigen Abhängigkeiten zwischen den einzelnen Bereichen sollten in der Leitlinie oder einem gesonderten Dokument dokumentiert werden.

5.1.2 Überprüfung der Informationssicherheitsleitlinie

Die in ISO/IEC 27002:2005, 5.1.2, empfohlenen Maßnahmen gelten entsprechend.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Handhabung der Informationssicherheit innerhalb der Organisation.

Ein Managementrahmen sollte geschaffen werden, um die Umsetzung der Informationssicherheit innerhalb der Organisation einzuführen und zu steuern.

Das Management sollte die Informationssicherheitsleitlinie genehmigen, sicherheitsbezogene Aufgaben zuweisen und die Umsetzung der Informationssicherheit organisationsweit koordinieren und überprüfen.

Bei Bedarf sollten spezifische Informationssicherheitsratschläge bereitgestellt und innerhalb der Organisation verfügbar gemacht werden. Kontakte zu externen Sicherheitsfachkräften oder -gruppen, einschließlich maßgeblicher Behörden, sollten hergestellt werden, um mit industriellen Entwicklungen Schritt zu halten, Normen und Bewertungsverfahren zu überwachen sowie geeignete Anlaufstellen zur Behandlung von Sicherheitsvorfällen zu schaffen. Eine interdisziplinäre Vorgehensweise bei der Informationssicherheit sollte gefördert werden.

6.1.1 Engagement des Managements für Informationssicherheit

Die in ISO/IEC 27002:2005, 6.1.1, empfohlenen Maßnahmen gelten entsprechend.

6.1.2 Koordinierung der Informationssicherheit

Die in ISO/IEC 27002:2005, 6.1.2, empfohlenen Maßnahmen gelten entsprechend.

6.1.3 Zuweisung von Verantwortlichkeiten hinsichtlich Informationssicherheit

Die in ISO/IEC 27002:2005, 6.1.3, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte einen Verantwortlichen benennen, der als Ansprechpartner für strategische Fragen zur Informationssicherheit Dritten zur Verfügung steht (z. B. für Planung und Umsetzung gemeinsamer Maßnahmen usw.).

6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen

Die in ISO/IEC 27002:2005, 6.1.4, empfohlenen Maßnahmen gelten entsprechend.

6.1.5 Vertraulichkeitsvereinbarungen

Die in ISO/IEC 27002:2005, 6.1.5, empfohlenen Maßnahmen gelten entsprechend.

6.1.6 Kontakt zu Behörden

Die in ISO/IEC 27002:2005, 6.1.6, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte mit den entsprechenden Fach- und Aufsichtsbehörden, insbesondere in den Bereichen IT-Sicherheit und Strafverfolgung und anderen kritischen Infrastrukturen zusammenarbeiten.

Das umfasst Kontakte zu Behörden, die sich mit dem Schutz kritischer Infrastrukturen auf nationaler und Europäischer Ebene beschäftigen.

6.1.7 Kontakte zu besonderen Interessengruppen

Die in ISO/IEC 27002:2005, 6.1.7, empfohlenen Maßnahmen gelten entsprechend.

Weitere für die Luftfahrt spezifische Informationen

Die Organisation sollte sich außerdem der Kritikalität ihrer Dienstleistungen auf regionaler, nationaler und internationaler Ebene bewusst sein. Sie darf sich deshalb in Verbänden und Zusammenschlüssen engagieren und sich an nationalen und internationalen Programmen beteiligen, um die Sicherheit im Luftverkehr umfassend zu unterstützen.

Aufgrund der besonderen Art der Bedrohungen für den Luftverkehr, kann es für die Organisation notwendig sein, mit anderen Luftverkehrsorganisationen zusammenzuarbeiten, um nach außen eine einmütige Position zu vertreten. Ein solcher gemeinsamer Auftritt sollte die Grundlage für die Auswahl angemessener Schutzmaßnahmen und reaktiver Maßnahmen sein:

- *Sicherstellung der Interoperabilität der ausgewählten Maßnahmen;*
- *Unterstützung der Zusammenarbeit bei der Alarmierung bei auftretenden IT-Krisen, die mehrere Organisationen betreffen, sowie bei der Krisen-Bewältigung;*
- *auf der Grundlage gemeinsam gezogener Lehren aus bereits aufgetretenen Sicherheitsvorfällen.*

6.1.8 Unabhängige Überprüfung der Informationssicherheit

Die in ISO/IEC 27002:2005, 6.1.8, empfohlenen Maßnahmen gelten entsprechend.

6.2 Externe Parteien

Ziel: Aufrechterhaltung der Sicherheit von Informationen und von informationsverarbeitenden Einrichtungen der Organisation, die für externe Parteien zugänglich sind, von ihnen verarbeitet oder verwaltet bzw. an sie kommuniziert werden.

Die Sicherheit von Informationen und informationsverarbeitenden Einrichtungen der Organisation sollte durch die Einführung von Produkten oder Dienstleistungen von externen Parteien nicht verringert werden.

Jeglicher Zugang, den externe Parteien zu den informationsverarbeitenden Einrichtungen der Organisation haben, sowie die Verarbeitung und Kommunikation von Informationen durch externe Parteien sollte überwacht werden.

Wenn es geschäftliche Gründe für die Zusammenarbeit mit externen Parteien gibt, die dazu möglicherweise auch Zugang zu den Informationen und informationsverarbeitenden Einrichtungen der Organisation benötigen, oder wenn ein Produkt und eine Dienstleistung von externen Parteien bereitgestellt oder ihnen zur Verfügung gestellt wird, so sollte eine Risikobewertung durchgeführt werden, um die Auswirkungen auf die Sicherheit und die Anforderungen an die Kontrollmaßnahmen zu ermitteln. Kontrollmaßnahmen sollten mit der betreffenden externen Partei vereinbart und in einer Vereinbarung festgelegt werden.

6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Parteien

Die in ISO/IEC 27002:2005, 6.2.1, empfohlenen Maßnahmen gelten entsprechend.

6.2.2 Behandlung von Sicherheit beim Umgang mit Kunden

Die in ISO/IEC 27002:2005, 6.2.2, empfohlenen Maßnahmen gelten entsprechend.

6.2.3 Behandlung von Sicherheit in Vereinbarungen mit Dritten

Die in ISO/IEC 27002:2005, 6.2.3, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Offenlegung von Identitäten gegenüber Partnern sollte Teil der Vereinbarungen sein. In den Vereinbarungen sollten die Bedingungen für die Offenlegung eindeutig festgelegt sein.

Bei Geschäftsprozessen, die mehrere Organisationen betreffen, sollte vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Werten (Assets) (siehe Abschnitt 7) festgelegt werden.

7 Management organisationseigener Werte (Assets)

7.1 Verantwortung für organisationseigene Werte (Assets)

Ziel: Erreichen und Erhalten eines angemessenen Schutzes von organisationseigenen Werten (Assets).

Alle organisationseigenen Werte (Assets) sollten ausgewiesen werden und einen benannten Eigentümer haben.

Für alle organisationseigenen Werte (Assets) sollten Eigentümer bestimmt werden, denen die Verantwortung für die Aufrechterhaltung angemessener Kontrollmaßnahmen obliegt. Gegebenenfalls darf der Eigentümer die Umsetzung bestimmter Kontrollmaßnahmen delegieren, er bleibt aber verantwortlich für den angemessenen Schutz der Werte.

7.1.1 Bestand organisationseigener Werte (Assets)

Die in ISO/IEC 27002:2005, 7.1.1, empfohlenen Maßnahmen gelten entsprechend.

7.1.2 Eigentum an organisationseigenen Werten (Assets)

Die in ISO/IEC 27002:2005, 7.1.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Wenn Werte in Geschäftsprozessen verwendet werden, an denen mehrere Organisationen beteiligt sind, sollten die Interessen der anderen Organisationen von den Eigentümern der Werte berücksichtigt werden.

7.1.3 Zulässige Nutzung von Werten

Die in ISO/IEC 27002:2005, 7.1.3, empfohlenen Maßnahmen gelten entsprechend.

7.2 Klassifizierung von Informationen

Ziel: Sicherstellung eines angemessenen Schutzes von Informationen.

Informationen sollten klassifiziert werden, um den Bedarf, die Prioritäten und den erwarteten Umfang des Schutzes bei der Nutzung der Informationen angeben zu können.

Informationen haben einen unterschiedlichen Grad von Sensitivität und Kritikalität. Manche Elemente können einen zusätzlichen Schutzgrad oder einen besonderen Umgang erfordern. Ein Klassifizierungsmodell für Informationen sollte zur Anwendung kommen, das eine angemessene Reihe von Schutzniveaus festlegt und den Bedarf an besonderen Maßnahmen zur Handhabung vermittelt.

7.2.1 Leitsätze für die Klassifizierung

Die in ISO/IEC 27002:2005, 7.2.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Um eine organisationsübergreifende Vergleichbarkeit sicherzustellen, sollte die Organisation Informationen, die in übergreifenden Geschäftsprozessen benutzt werden, so klassifizieren, dass diese Klassifizierung für alle am Geschäftsprozess beteiligten Partner annehmbar ist und sie dieser Klassifizierung zustimmen. Derartige Informationen sollten klassifiziert werden, um sicherzustellen, dass nationale und geschäftliche Interessen in angemessener Weise geschützt werden.

Vertraulichkeitsklassen:

Die Zuordnung von Informationen zu einer Vertraulichkeitsklasse sollte auf der Grundlage des zu erwartenden Schadens für den Geschäftsprozess, falls die Information Unberechtigten zur Kenntnis gelangt, erfolgen.

Öffentlich: Informationen, deren Bekanntwerden keinen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich zieht

Intern: Informationen, deren Bekanntwerden einen geringen bis mittleren Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich zieht

Vertraulich: Informationen, deren Bekanntwerden einen großen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann

Streng Vertraulich: Informationen, deren Bekanntwerden einen erheblichen bis existenziellen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann

Allgemein sollte die gemeinsame Nutzung von Informationen nach dem „Need-to-know-Prinzip“ erfolgen.

Weitere für die Luftfahrt spezifische Informationen

Geschäftliche Bedürfnisse und die geschäftlichen Auswirkungen in Zusammenhang mit diesen Bedürfnissen können das öffentliche Interesse an einer sicheren und schnellen Erbringung der Dienstleistung einschließen wie auch geschäftliche Interessen von einzelnen Beteiligten.

7.2.2 Kennzeichnung von und Umgang mit Informationen

Die in ISO/IEC 27002:2005, 7.2.2, empfohlenen Maßnahmen gelten entsprechend.

8 Sicherheit personeller Ressourcen

8.1 Vor der Einstellung

Ziel: Sicherstellung, dass Angestellte, Auftragnehmer und Drittbenutzer ihre Verantwortlichkeiten verstehen und für die vorgesehenen Aufgaben geeignet sind, sowie Verringerung des Risikos von Diebstahl, Betrug oder Missbrauch von Einrichtungen.

Die Verantwortlichkeiten für Sicherheit sollte vor der Einstellung in entsprechenden Stellenbeschreibungen und Beschäftigungsbedingungen behandelt werden.

Alle Bewerber für eine Anstellung, Auftragnehmer und Drittbenutzer sollten angemessen überprüft werden, insbesondere, wenn sie für sensible Stellen eingesetzt werden sollen.

Angestellte, Auftragnehmer und Drittbenutzer von informationsverarbeitenden Einrichtungen sollten eine Vereinbarung bezüglich ihrer Sicherheitsaufgaben und -verantwortlichkeiten unterschreiben.

8.1.1 Aufgaben und Verantwortlichkeiten

Die in ISO/IEC 27002:2005, 8.1.1, empfohlenen Maßnahmen gelten entsprechend.

8.1.2 Überprüfung

Die in ISO/IEC 27002:2005, 8.1.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Im Falle mehrerer Partnerorganisationen sollte sichergestellt sein, dass von Partnerorganisationen Hintergrundüberprüfungen auf einem angemessenen Niveau durchgeführt werden, um sicherzustellen, dass der Zugriff auf Daten/Informationen, die von den Partnerorganisationen gemeinsam genutzt werden, die nationalen und geschäftlichen Interessen aller Beteiligten berücksichtigt.

8.1.3 Beschäftigungsbedingungen

Die in ISO/IEC 27002:2005, 8.1.3, empfohlenen Maßnahmen gelten entsprechend.

8.2 Während der Anstellung

Ziel: Sicherstellung, dass Angestellte, Auftragnehmer und Drittbenutzer die Informationssicherheitsbedrohungen und -bedenken sowie ihre Verantwortlichkeiten und Pflichten kennen, und dass sie entsprechend ausgestattet sind, die organisationseigene Sicherheitsleitlinie bei ihrer üblichen Arbeit zu befolgen, und das Risiko von menschlichen Fehlern zu reduzieren.

Die Verantwortlichkeiten des Managements sollte festgelegt werden, um sicherzustellen, dass Sicherheit während des gesamten Beschäftigungsverhältnisses einer Person in der Organisation zur Anwendung kommt.

Ein angemessenes Niveau bezüglich des Bewusstseins, der Ausbildung und Schulung in Sicherheitsverfahren und der ordnungsgemäßen Nutzung von informationsverarbeitenden Einrichtungen sollte allen Angestellten, Auftragnehmern und Drittbenutzern vermittelt werden, um mögliche Sicherheitsrisiken gering zu halten. Für die Behandlung von Sicherheitsverstößen sollte ein formales Disziplinarverfahren eingerichtet werden.

8.2.1 Verantwortung des Managements

Die in ISO/IEC 27002:2005, 8.2.1, empfohlenen Maßnahmen gelten entsprechend.

8.2.2 Bewusstsein, Bildung und Schulung bezüglich der Informationssicherheit

Die in ISO/IEC 27002:2005, 8.2.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Herausbildung des Bewusstseins der Angestellten, ihre Ausbildung und Schulung bezüglich Informationssicherheit sollte insbesondere in Übereinstimmung mit den maßgeblichen Festlegungen der Dokumente der Internationalen Zivilluftfahrtorganisation (ICAO) erfolgen.

Die Organisation sollte sicherstellen, dass Anwendungsentwickler über Fähigkeiten verfügen, die es ihnen ermöglichen, sichere Anwendungen umzusetzen.

8.2.3 Disziplinarverfahren

Die in ISO/IEC 27002:2005, 8.2.3, empfohlenen Maßnahmen gelten entsprechend.

8.3 Beendigung oder Wechsel der Anstellung

Ziel: Sicherstellung, dass Angestellte, Auftragnehmer und Drittbenuztzer ordnungsgemäß die Organisation verlassen oder die Anstellung wechseln.

Verantwortlichkeiten sollten etabliert werden, um sicherzustellen, dass Angestellte, Auftragnehmer oder Drittbenuztzer die Organisation in geregelter Weise verlassen, und dass die Rückgabe aller Geräte und das Entfernen aller Zugangsrechte abgeschlossen sind.

Änderungen von Verantwortlichkeiten und Anstellungen innerhalb einer Organisation sollten genauso behandelt werden wie die Beendigung der jeweiligen Verantwortlichkeit oder des Beschäftigungsverhältnisses in Übereinstimmung mit diesem Abschnitt, und alle Neuanstellungen sollten wie in 8.1 beschrieben behandelt werden.

8.3.1 Verantwortlichkeiten bei der Beendigung

Die in ISO/IEC 27002:2005, 8.3.1, empfohlenen Maßnahmen gelten entsprechend.

8.3.2 Rückgabe von organisationseigenen Werten (Assets)

Die in ISO/IEC 27002:2005, 8.3.2, empfohlenen Maßnahmen gelten entsprechend.

8.3.3 Aufhebung von Zugangsrechten

Die in ISO/IEC 27002:2005, 8.3.3, empfohlenen Maßnahmen gelten entsprechend.

9 Physische und umgebungsbezogene Sicherheit

9.1 Sicherheitsbereiche

Ziel: Schutz vor dem Zugang zu, der Beschädigung und Störung des Geländes der Organisation sowie von der Organisation gehörenden Informationen durch Unbefugte.

Kritische oder sensible informationsverarbeitende Einrichtungen sollten in Sicherheitsbereichen untergebracht sein, welche durch festgelegte Sicherheitszonen mit angemessenen Sicherheitsbarrieren und Zugangskontrollsystemen geschützt sind. Sie sollten physisch vor dem Zugang, der Beschädigung und Störung durch Unbefugte geschützt sein.

Der vorgesehene Schutz sollte entsprechend den identifizierten Risiken erfolgen.

9.1.1 Physische Sicherheitszonen

Die in ISO/IEC 27002:2005, 9.1.1, empfohlenen Maßnahmen gelten entsprechend.

9.1.2 Physische Zugangskontrollen

Die in ISO/IEC 27002:2005, 9.1.2, empfohlenen Maßnahmen gelten entsprechend.

9.1.3 Sicherung von Büros, Räumen und Einrichtungen

Die in ISO/IEC 27002:2005, 9.1.3, empfohlenen Maßnahmen gelten entsprechend.

9.1.4 Schutz vor Bedrohungen von außen und aus der Umgebung

Die in ISO/IEC 27002:2005, 9.1.4, empfohlenen Maßnahmen gelten entsprechend.

9.1.5 Arbeit in Sicherheitsbereichen

Die in ISO/IEC 27002:2005, 9.1.5, empfohlenen Maßnahmen gelten entsprechend.

9.1.6 Öffentlicher Zugang, Anlieferungs- und Ladebereiche

Die in ISO/IEC 27002:2005, 9.1.6, empfohlenen Maßnahmen gelten entsprechend.

9.2 Sicherheit von Ausrüstungen

Ziel: Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Tätigkeiten einer Organisation.

Ausrüstungen sollten vor physischen Bedrohungen und Bedrohungen aus der Umgebung geschützt werden.

Es ist notwendig, die Ausrüstungen (auch diejenigen, die außerhalb der Einrichtungen eingesetzt werden sowie die Entfernung von Eigentum) zu schützen, um so das Risiko des unbefugten Zugriffs auf Informationen zu verringern. Dabei sollten ebenfalls die Standortwahl und die Entsorgung von Ausrüstungen in Betracht gezogen werden. Spezielle Kontrollmaßnahmen können notwendig werden, um Ausrüstungen vor physischen Bedrohungen zu schützen und die unterstützenden Einrichtungen, wie z. B. die Stromversorgung und die Verkabelung, zu schützen.

9.2.1 Standortwahl und Schutz von Ausrüstungen

Die in ISO/IEC 27002:2005, 9.2.1, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Ausrüstungen, die in öffentlich zugänglichen Bereichen eingesetzt werden, sollten gegen unberechtigten Zugriff geschützt werden, z. B. durch feststehende und abzusperrende Gehäuse für PCs, physische und/oder logische Absicherung von Netzwerkdozen usw.

9.2.2 Unterstützende Versorgungseinrichtungen

Die in ISO/IEC 27002:2005, 9.2.2, empfohlenen Maßnahmen gelten entsprechend.

9.2.3 Sicherheit der Verkabelung

Die in ISO/IEC 27002:2005, 9.2.3, empfohlenen Maßnahmen gelten entsprechend.

9.2.4 Instandhaltung von Ausrüstungen

Die in ISO/IEC 27002:2005, 9.2.4, empfohlenen Maßnahmen gelten entsprechend.

9.2.5 Sicherheit von außerhalb des Standortes eingesetzten Ausrüstungen

Die in ISO/IEC 27002:2005, 9.2.5, empfohlenen Maßnahmen gelten entsprechend.

9.2.6 Sichere Entsorgung oder Wiederverwendung von Ausrüstungen

Die in ISO/IEC 27002:2005, 9.2.6, empfohlenen Maßnahmen gelten entsprechend.

9.2.7 Entfernung von Eigentum

Die in ISO/IEC 27002:2005, 9.2.7, empfohlenen Maßnahmen gelten entsprechend.

10 Kommunikations- und Betriebsmanagement

10.1 Den Betrieb betreffende Verfahren und Verantwortlichkeiten

Ziel: Sicherstellung des ordnungsgemäßen und sicheren Betriebs der informationsverarbeitenden Einrichtungen.

Für das Management und den Betrieb aller informationsverarbeitenden Einrichtungen sollten Verantwortlichkeiten und Verfahrensweisen festgelegt werden. Dies beinhaltet die Entwicklung angemessener Betriebsabläufe.

Die Aufteilung von Pflichten sollte gegebenenfalls umgesetzt werden, um so das Risiko von fahrlässigem oder vorsätzlichem Missbrauch des Systems zu verringern.

10.1.1 Dokumentierte Betriebsabläufe

Die in ISO/IEC 27002:2005, 10.1.1, empfohlenen Maßnahmen gelten entsprechend.

10.1.2 Verwaltung von Änderungen

Die in ISO/IEC 27002:2005, 10.1.2, empfohlenen Maßnahmen gelten entsprechend.

10.1.3 Aufteilung von Pflichten

Die in ISO/IEC 27002:2005, 10.1.3, empfohlenen Maßnahmen gelten entsprechend.

10.1.4 Aufteilung von Entwicklungs- und Prüfeinrichtungen und Betriebsanlagen

Die in ISO/IEC 27002:2005, 10.1.4, empfohlenen Maßnahmen gelten entsprechend.

10.2 Management der Erbringung von Dienstleistungen durch Dritte

Ziel: Umsetzung und Aufrechterhaltung eines angemessenen Grads an Informationssicherheit und Erbringung von Dienstleistungen in Übereinstimmung mit den Liefervereinbarungen mit Dritten.

Die Organisation sollte die Umsetzung von Vereinbarungen überprüfen, die Übereinstimmung mit den Vereinbarungen überwachen und Änderungen verwalten, um sicherzustellen, dass die erbrachten Dienstleistungen alle mit den Dritten vereinbarten Anforderungen erfüllen.

10.2.1 Erbringung von Dienstleistungen

Die in ISO/IEC 27002:2005, 10.2.1, empfohlenen Maßnahmen gelten entsprechend.

10.2.2 Überwachung und Überprüfung von durch Dritte erbrachten Dienstleistungen

Die in ISO/IEC 27002:2005, 10.2.2, empfohlenen Maßnahmen gelten entsprechend.

10.2.3 Management von Änderungen an durch Dritte erbrachten Dienstleistungen

Die in ISO/IEC 27002:2005, 10.2.3, empfohlenen Maßnahmen gelten entsprechend.

10.3 Systemplanung und Abnahme

Ziel: Das Risiko von Systemausfällen gering zu halten.

Vorausschauende Planung und Vorbereitung sind erforderlich, um sicherzustellen, dass angemessene Kapazitäten und Ressourcen verfügbar bleiben, um die geforderte Systemleistung zu erbringen.

Um das Risiko von Systemüberlastungen zu verringern, sollten Abschätzungen für zukünftige Kapazitätsanforderungen durchgeführt werden.

Die Betriebsanforderungen an neue Systeme sollten festgelegt, dokumentiert und geprüft werden, bevor diese abgenommen und benutzt werden.

10.3.1 Kapazitätsmanagement

Die in ISO/IEC 27002:2005, 10.3.1, empfohlenen Maßnahmen gelten entsprechend.

10.3.2 System-Abnahme

Die in ISO/IEC 27002:2005, 10.3.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Abnahme von Systemen, die in organisationsübergreifenden Prozessen eingesetzt werden, sollte einen formalen Prozess beinhalten, der sicherstellt, dass die Systemabnahme-Anforderungen und -kriterien mit der in Abschnitt 4 beschriebenen gemeinsamen Risikobewertung in Einklang stehen.

10.4 Schutz vor Schadsoftware und mobilen Programmcodes

Ziel: Schutz der Integrität von Software und Informationen.

Vorsichtsmaßnahmen sind notwendig, um das Einschleusen von Schadsoftware und nicht genehmigtem mobilen Programmcodes zu verhindern und zu erkennen.

Software und informationsverarbeitende Einrichtungen sind für das Einschleusen von Schadsoftware wie Computer-Viren, Würmern, trojanischen Pferden und logischen Bomben anfällig. Die Benutzer sollten auf die Gefahren durch Schadsoftware hingewiesen werden. Manager sollten, soweit erforderlich, Maßnahmen zum Schutz vor, bzw. zum Erkennen und Entfernen von Schadsoftware und zur Steuerung von mobilen Programmcodes treffen.

10.4.1 Maßnahmen gegen Schadsoftware

Die in ISO/IEC 27002:2005, 10.4.1, empfohlenen Maßnahmen gelten entsprechend.

10.4.2 Maßnahmen gegen mobile Programmcodes

Die in ISO/IEC 27002:2005, 10.4.2, empfohlenen Maßnahmen gelten entsprechend.

10.5 Backup

Ziel: Erhaltung der Integrität und der Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen.

Routineverfahren sollten etabliert werden, die die vereinbarte Backup-Verfahrensweise und Strategie (siehe auch 14.1) umsetzen, Backup-Kopien von Daten erstellen und Proben eines rechtzeitigen Wiedereinspielens durchführen.

10.5.1 Backup von Informationen

Die in ISO/IEC 27002:2005, 10.5.1, empfohlenen Maßnahmen gelten entsprechend.

10.6 Management der Netzsicherheit

Ziel: Sicherstellung des Schutzes von Informationen in Netzen sowie Schutz der unterstützenden Infrastruktur.

Das sichere Management von Netzen, die Organisationsgrenzen überspannen können, erfordert sorgfältige Überlegungen über den Datenfluss, die rechtlichen Auswirkungen, die Überwachung und den Schutz.

Zum Schutz sensibler Informationen die über öffentliche Netze transportiert werden, können außerdem zusätzliche Maßnahmen erforderlich sein.

10.6.1 Maßnahmen für Netze

Die in ISO/IEC 27002:2005, 10.6.1, empfohlenen Maßnahmen gelten entsprechend.

10.6.2 Sicherheit von Netzdiensten

Die in ISO/IEC 27002:2005, 10.6.2, empfohlenen Maßnahmen gelten entsprechend.

10.7 Umgang mit Medien

Ziel: Die unerlaubte Veröffentlichung, Veränderung, Entnahme oder Zerstörung von organisationseigenen Werten (Assets) sowie die Unterbrechung der Geschäftstätigkeit zu verhindern.

Speichermedien sollten kontrolliert und physisch geschützt werden.

Angemessene Betriebsabläufe sollten etabliert werden, um Dokumente, Speicher-Medien (z. B. Bänder, Disketten), Ein-/Ausgabedaten und Systemdokumentation vor unerlaubter Veröffentlichung, Veränderung, Entnahme und Zerstörung zu schützen.

10.7.1 Management von austauschbaren Medien

Die in ISO/IEC 27002:2005, 10.7.1, empfohlenen Maßnahmen gelten entsprechend.

10.7.2 Entsorgung von Medien

Die in ISO/IEC 27002:2005, 10.7.2, empfohlenen Maßnahmen gelten entsprechend.

10.7.3 Verfahren für den Umgang mit Informationen

Die in ISO/IEC 27002:2005, 10.7.3, empfohlenen Maßnahmen gelten entsprechend.

10.7.4 Sicherheit der Systemdokumentation

Die in ISO/IEC 27002:2005, 10.7.4, empfohlenen Maßnahmen gelten entsprechend.

10.8 Austausch von Informationen

Ziel: Aufrechterhaltung der Sicherheit von Informationen und Software, die innerhalb einer Organisation oder mit Externen ausgetauscht werden.

Der Austausch von Informationen und Software zwischen Organisationen sollte auf einem formalen Regelwerk basieren und im Einklang mit den Austauschvereinbarungen durchgeführt werden, und sollte mit allen maßgeblichen gesetzlichen Festlegungen übereinstimmen (siehe Abschnitt 15).

Verfahren und Normen sollten festgelegt werden, um Informationen und physische Medien, die Informationen enthalten, während des Transports zu schützen.

10.8.1 Regelwerke und Verfahren für den Austausch von Informationen

Die in ISO/IEC 27002:2005, 10.8.1, empfohlenen Maßnahmen gelten entsprechend.

10.8.2 Vereinbarungen zum Austausch von Informationen

Die in ISO/IEC 27002:2005, 10.8.2, empfohlenen Maßnahmen gelten entsprechend.

10.8.3 Physische Medien während des Transports

Die in ISO/IEC 27002:2005, 10.8.3, empfohlenen Maßnahmen gelten entsprechend.

10.8.4 Elektronische Übermittlung von Mitteilungen

Die in ISO/IEC 27002:2005, 10.8.4, empfohlenen Maßnahmen gelten entsprechend.

10.8.5 Geschäftsinformationssysteme

Die in ISO/IEC 27002:2005, 10.8.5, empfohlenen Maßnahmen gelten entsprechend.

10.9 Dienstleistungen im Rahmen des elektronischen Geschäftsverkehrs

Ziel: Sicherstellung der Sicherheit von Dienstleistungen im Rahmen des elektronischen Geschäftsverkehrs und ihrer sicheren Nutzung.

Die mit der Nutzung von Dienstleistungen im Rahmen des elektronischen Geschäftsverkehrs einschließlich Online-Transaktionen verbundenen Auswirkungen auf die Sicherheit und Anforderungen an entsprechende Maßnahmen sollten bedacht werden. Die Integrität und Verfügbarkeit von elektronisch bereitgestellten Informationen mittels öffentlich zugänglicher Systeme sollte ebenfalls bedacht werden.

10.9.1 Elektronischer Geschäftsverkehr

Die in ISO/IEC 27002:2005, 10.9.1, empfohlenen Maßnahmen gelten entsprechend.

10.9.2 Online-Transaktionen

Die in ISO/IEC 27002:2005, 10.9.2, empfohlenen Maßnahmen gelten entsprechend.

10.9.3 Öffentlich verfügbare Informationen

Die in ISO/IEC 27002:2005, 10.9.3, empfohlenen Maßnahmen gelten entsprechend.

10.10 Überwachung

Ziel: Entdeckung informationsverarbeitender Tätigkeiten durch Unbefugte.

Systeme sollten überwacht und Informationssicherheitsereignisse sollten aufgezeichnet werden. Protokollierungen der Administrationstätigkeiten und von Fehlern sollten dazu genutzt werden sicherzustellen, dass Probleme bei Informationssystemen identifiziert werden.

Eine Organisation sollte alle maßgeblichen gesetzlichen Anforderungen an die Überwachung und Protokollierung erfüllen.

Systemüberwachung sollte dazu genutzt werden, die Wirksamkeit der getroffenen Maßnahmen zu überprüfen und die Konformität mit einer Zugriffskontrollregelung zu verifizieren.

10.10.1 Protokollierung von Audits

Die in ISO/IEC 27002:2005, 10.10.1, empfohlenen Maßnahmen gelten entsprechend.

10.10.2 Überwachung der Systemnutzung

Die in ISO/IEC 27002:2005, 10.10.2, empfohlenen Maßnahmen gelten entsprechend.

10.10.3 Schutz von Protokollinformationen

Die in ISO/IEC 27002:2005, 10.10.3, empfohlenen Maßnahmen gelten entsprechend.

10.10.4 Administrator- und Betreiberprotokolle

Die in ISO/IEC 27002:2005, 10.10.4, empfohlenen Maßnahmen gelten entsprechend.

10.10.5 Fehlerprotokollierung

Die in ISO/IEC 27002:2005, 10.10.5, empfohlenen Maßnahmen gelten entsprechend.

10.10.6 Zeitsynchronisierung

Die in ISO/IEC 27002:2005, 10.10.6, empfohlenen Maßnahmen gelten entsprechend.

11 Zugangskontrolle

11.1 Geschäftsanforderungen an die Zugangskontrolle

Ziel: Kontrolle des Zugangs zu Informationen.

Der Zugang zu Informationen, informationsverarbeitenden Einrichtungen und Geschäftsprozessen sollte auf der Grundlage von Geschäfts- und Sicherheitsanforderungen kontrolliert werden.

Regeln für die Zugangskontrolle sollten Leitlinien für die Verbreitung von Informationen und für deren Autorisierung berücksichtigen.

11.1.1 Leitlinie für die Zugangskontrolle

Die in ISO/IEC 27002:2005, 11.1.1, empfohlenen Maßnahmen gelten entsprechend.

11.2 Benutzerverwaltung

Ziel: Sicherstellung, dass Informationssysteme für befugte Benutzer zugänglich und für Unbefugte unzugänglich sind.

Formale Verfahren zur Kontrolle der Zuweisung von Zugangsrechten zu Informationssystemen und Diensten sollten etabliert sein.

Die Verfahren sollten alle Stadien im Lebenszyklus des Benutzerzugangs, von der erstmaligen Registrierung als neuer Benutzer bis zur endgültigen Löschung von Benutzern, die keinen Zugang mehr zu Informationssystemen und Diensten benötigen, abdecken. Besondere Aufmerksamkeit sollte soweit angemessen der Kontrolle der Zuweisung von bevorzugten Zugangsrechten gewidmet werden, die es den Benutzern erlauben, Systemkontrollen zu überwinden.

11.2.1 Benutzerregistrierung

Die in ISO/IEC 27002:2005, 11.2.1, empfohlenen Maßnahmen gelten entsprechend.

11.2.2 Privilegmanagement

Die in ISO/IEC 27002:2005, 11.2.2, empfohlenen Maßnahmen gelten entsprechend.

11.2.3 Verwaltung von Benutzerpasswörtern

Die in ISO/IEC 27002:2005, 11.2.3, empfohlenen Maßnahmen gelten entsprechend.

11.2.4 Überprüfung der Zugangsrechte von Benutzern

Die in ISO/IEC 27002:2005, 11.2.4, empfohlenen Maßnahmen gelten entsprechend.

11.2.5 Digitales Identitätsmanagement

Maßnahme

Zur Verwaltung digitaler Identitäten, ihrer Authentisierung, Autorisierung, Rollen und Rechte sollte die Organisation ein zentrales Identitätsmanagementsystem betreiben. Die Gültigkeit einer Identität sollte nachvollziehbar in Bezug auf das Quellsystem der Identität vorgegeben sein.

Anleitung für die Umsetzung

Quellendatenbanken (z. B. LDAP-Verzeichnisse, Active Directory, dezentrale Datenbanken wie SAP usw.) des Identitätsmanagementsystems sollten eine eindeutige Beziehung zwischen einer Identität und einer Entität des zentralen Identitätsmanagementsystems herstellen.

Die folgenden Hauptprozesse zur Verwaltung digitaler Identitäten sollten umgesetzt werden:

- Erzeugung digitaler Identitäten;
- Änderung (Anpassung, Erweiterung, Löschung) von Merkmalen einer digitalen Identität;
- Deaktivierung/Löschung digitaler Identitäten;
- systematische Bereitstellung digitaler Identitätsinformationen (einschließlich Authentisierungsdaten) für angeschlossene Systeme;
- Verarbeitung von Informationen (aus der Personalverwaltung und dem Organisationsmanagement) zur automatisierten Verwaltung von Benutzergruppen, Rollen und Rechten (Autorisierungsprofile);
- systematische Bereitstellung von Benutzergruppen, Rollen und Rechten in angeschlossenen Systemen.

Jeder der vorgenannten Prozesse im Zusammenhang mit dem digitalen Identitäts-Management sollte dokumentiert werden und rückverfolgbar sein.

Die Gültigkeit sollte durch ein angeschlossenes Personalmanagementsystem oder über ein verbundenes Unternehmensverzeichnis umgesetzt werden.

Sofern manuelle Prozesse angewendet werden müssen, sollte die Gültigkeitsdauer ein Jahr nicht überschreiten. Die Festlegung einer neuen Gültigkeitsdauer sollte einmal jährlich durch eine Überprüfung erfolgen.

11.2.6 Organisationsübergreifende eindeutige Darstellung von Entitäten

Maßnahme

Im organisationsübergreifenden Identitätsmanagement sollten folgende Entitäten betrachtet werden:

- Menschen;
- Organisationseinheiten (z. B. Abteilungen) und organisatorische Rollen;
- Systeme.

Jede Entität der Organisation sollte im zentralen Identitätsmanagementsystem durch eine eindeutige digitale Identität dargestellt werden.

Weitere Informationen

Ein einheitliches System zur organisationsübergreifenden Darstellung von Entitäten stellt die Kompatibilität und Interoperabilität im Identitätsmanagement sicher.

11.3 Benutzerverantwortung

Ziel: Verhindern von unbefugtem Benutzerzugriff, Kompromittierung oder Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

Die Mitarbeit der befugten Benutzer ist für eine wirksame Sicherheit von grundlegender Bedeutung.

Benutzer sollten sich ihrer Verantwortung für die Aufrechterhaltung wirksamer Zugangskontrollen, besonders im Hinblick auf die Verwendung von Passwörtern und die Sicherheit von Benutzergeräten, bewusst sein.

Der Grundsatz der leeren/aufgeräumten Schreibtische und des leeren Bildschirms (en: clean desk and clean screen) sollte umgesetzt werden, um das Risiko des Zugangs durch Unbefugte, oder der Beschädigung von Unterlagen, Informationsträgern und informationsverarbeitenden Einrichtungen zu verringern.

11.3.1 Verwendung von Passwörtern

Die in ISO/IEC 27002:2005, 11.3.1, empfohlenen Maßnahmen gelten entsprechend.

11.3.2 Unbeaufsichtigte Benutzergeräte

Die in ISO/IEC 27002:2005, 11.3.2, empfohlenen Maßnahmen gelten entsprechend.

11.3.3 Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

Die in ISO/IEC 27002:2005, 11.3.3, empfohlenen Maßnahmen gelten entsprechend.

11.4 Zugangskontrolle für Netze

Ziel: Verhinderung von unbefugtem Zugang zu Netzdiensten.

Der Zugang sowohl zu internen als auch zu externen Netzdiensten sollte gesteuert werden.

Der Benutzerzugang zu Netzen und Netzdiensten sollte die Sicherheit der Netzdienste nicht kompromittieren, indem sichergestellt wird, dass:

- a) angemessene Schnittstellen zwischen dem Netz der Organisation und Netzen, die anderen Organisationen gehören, sowie öffentlich zugänglichen Netzen vorhanden sind;
- b) angemessene Mechanismen zur Authentisierung von Benutzern und Geräten angewendet werden;
- c) die Zugangs- und Zugriffskontrolle für Benutzer von Informationsdiensten erzwungen wird.

11.4.1 Regelwerk zur Nutzung von Netzdiensten

Die in ISO/IEC 27002:2005, 11.4.1, empfohlenen Maßnahmen gelten entsprechend.

11.4.2 Benutzerauthentisierung für externe Verbindungen

Die in ISO/IEC 27002:2005, 11.4.2, empfohlenen Maßnahmen gelten entsprechend.

11.4.3 Geräteidentifizierung in Netzen

Die in ISO/IEC 27002:2005, 11.4.3, empfohlenen Maßnahmen gelten entsprechend.

11.4.4 Schutz von Ferndiagnose- und Konfigurations-Ports

Die in ISO/IEC 27002:2005, 11.4.4, empfohlenen Maßnahmen gelten entsprechend.

11.4.5 Trennung in Netzwerken

Die in ISO/IEC 27002:2005, 11.4.5, empfohlenen Maßnahmen gelten entsprechend.

11.4.6 Steuerung von Netzverbindungen

Die in ISO/IEC 27002:2005, 11.4.6, empfohlenen Maßnahmen gelten entsprechend.

11.4.7 Routingkontrolle für Netze

Die in ISO/IEC 27002:2005, 11.4.7, empfohlenen Maßnahmen gelten entsprechend.

11.5 Steuerung des Zugriffs auf Betriebssysteme

Ziel: Verhinderung des unbefugten Zugriffs auf Betriebssysteme.

Sicherheitseinrichtungen sollten dazu genutzt werden, den Zugriff auf Betriebssysteme auf befugte Benutzer zu beschränken. Die Einrichtungen sollten die folgenden Fähigkeiten haben:

- a) Authentisierung befugter Benutzer in Übereinstimmung mit einem festgelegten Regelwerk für die Zugangskontrolle;
- b) Aufzeichnung von erfolgreichen und fehlgeschlagenen Authentisierungsversuchen;
- c) Aufzeichnung der Verwendung spezieller Systemberechtigungen;
- d) Alarmierung, wenn die Sicherheitsregelungen des Systems verletzt werden;
- e) Bereitstellung angemessener Funktionen zur Authentisierung;
- f) Gegebenenfalls Einschränkung der Sitzungsdauer von Benutzern.

11.5.1 Verfahren zur sicheren Anmeldung

Die in ISO/IEC 27002:2005, 11.5.1, empfohlenen Maßnahmen gelten entsprechend.

11.5.2 Identifizierung und Authentisierung von Benutzern

Die in ISO/IEC 27002:2005, 11.5.2, empfohlenen Maßnahmen gelten entsprechend.

11.5.3 Passwort-Verwaltungssystem

Die in ISO/IEC 27002:2005, 11.5.3, empfohlenen Maßnahmen gelten entsprechend.

11.5.4 Verwendung von Systemwerkzeugen

Die in ISO/IEC 27002:2005, 11.5.4, empfohlenen Maßnahmen gelten entsprechend.

11.5.5 Automatische Beendigung der Sitzung

Die in ISO/IEC 27002:2005, 11.5.5, empfohlenen Maßnahmen gelten entsprechend.

11.5.6 Begrenzung der Verbindungszeit

Die in ISO/IEC 27002:2005, 11.5.6, empfohlenen Maßnahmen gelten entsprechend.

11.6 Zugangskontrolle für Anwendungen und Informationen

Ziel: Verhinderung des unbefugten Zugangs zu Informationen, die in Anwendungssystemen bereitgestellt werden.

Sicherheitseinrichtungen sollten dazu genutzt werden, den Zugang zu und innerhalb von Anwendungssystemen zu beschränken.

Logischer Zugang zu Anwendungssoftware und Informationen sollte auf berechnigte Benutzer beschränkt sein.

Anwendungssysteme sollten:

- a) den Benutzerzugang zu Informationen und Funktionen des Anwendungssystems nach dem festgelegten Regelwerk zur Zugangskontrolle kontrollieren;
- b) Schutz vor unbefugtem Zugriff durch Werkzeuge, Betriebssystemsoftware und Schadsoftware bieten, die in der Lage sind, System- und Anwendungskontrollen zu überwinden oder zu umgehen.
- c) andere Systeme, mit denen Informationsressourcen geteilt werden, nicht kompromittieren.

11.6.1 Beschränkung des Zugriffs auf Informationen

Die in ISO/IEC 27002:2005, 11.6.1, empfohlenen Maßnahmen gelten entsprechend.

11.6.2 Isolierung sensibler Systeme

Die in ISO/IEC 27002:2005, 11.6.2, empfohlenen Maßnahmen gelten entsprechend.

11.6.3 Web-Application Firewalls

Maßnahme

Die Organisation sollte zum Schutz von Web-Anwendungen Web-Application Firewalls einsetzen.

Anleitung zur Umsetzung

Um versuchte Angriffe auf Web-Anwendungen vorausschauend erkennen, protokollieren und abblocken zu können, sollte die nachstehende Anleitung für die Umsetzung befolgt werden:

- eine Basis von Signaturen (oder Rollen), die verbreitete Angriffe wie z. B. seitenübergreifendes Scripting (XSS) und SQL-Einschleusung abdecken, sollte angewendet und auf dem aktuellen Stand gehalten werden;
- Angriff-Signaturen (oder Rollen) sollten für jede Web-Anwendung angepasst werden und bei Änderungen an den Anwendungen auf dem aktuellen Stand gehalten werden.

Weitere Informationen

Eine Application Firewall ist eine Art Firewall, die den Eintritt, Austritt und/oder den Zugang von, zu oder durch eine Anwendung oder einen Dienst steuert. Sie funktioniert durch Überwachung und möglicherweise Blockierung des Eintritts, Austritts oder von System Service Calls, die nicht mit der konfigurierten Leitlinie übereinstimmen. Die Web-Application-Firewall-Technik verfügt speziell über die Fähigkeit, eine Reihe von Rollen auf HTTP/HTTPS-Nachrichtenübermittlungen anzuwenden, um viele Angriffsversuche erkennen und blockieren zu können.

11.7 Mobile Computing und Telearbeit

Ziel: Sicherstellung der Informationssicherheit bei der Benutzung von Einrichtungen für Mobile Computing und Telearbeit.

Der erforderliche Schutz sollte im Einklang mit den Risiken dieser speziellen Arten von Arbeiten stehen.

Wird Mobile Computing angewendet, so sollten die Risiken, die durch die Arbeit in ungeschützten Umgebungen entstehen, berücksichtigt und angemessene Schutzmaßnahmen getroffen werden. Im Fall der Telearbeit sollte die Organisation den Schutz des Telearbeitsplatzes sicherstellen und dafür sorgen, dass angemessene Vorkehrungen für diese Art der Arbeit getroffen worden sind.

11.7.1 Mobile Computing und Kommunikation

Die in ISO/IEC 27002:2005, 11.7.1, empfohlenen Maßnahmen gelten entsprechend.

11.7.2 Telearbeit

Die in ISO/IEC 27002:2005, 11.7.2, empfohlenen Maßnahmen gelten entsprechend.

12 Beschaffung, Entwicklung und Aufrechterhaltung von Informationssystemen

12.1 Sicherheitsanforderungen an Informationssysteme

Ziel: Sicherzustellen, dass Sicherheit ein fester Bestandteil von Informationssystemen ist.

Informationssysteme beinhalten Betriebssysteme, Infrastruktur, Geschäftsanwendungen, Standardprodukte, Dienste und von Benutzern entwickelte Anwendungen. Die Gestaltung und Umsetzung von Informationssystemen, die Geschäftsprozesse unterstützen, können für die Sicherheit von entscheidender Bedeutung sein. Sicherheitsanforderungen sollten vor der Entwicklung und/oder Umsetzung von Informationssystemen identifiziert und vereinbart werden.

Alle Sicherheitsanforderungen sollten während der Phase der Anforderungsfestlegung eines Projektes identifiziert, begründet, vereinbart und als Teil des Geschäftsmodells des Informationssystems dokumentiert werden.

12.1.1 Analyse und Festlegung von Sicherheitssanforderungen

Die in ISO/IEC 27002:2005, 12.1.1, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Sicherheitsanforderungen und -maßnahmen sollten die Sicherheitsanforderungen der betroffenen externen Organisationen, die an gemeinsamen Geschäftsprozessen beteiligt sind, berücksichtigen.

12.1.2 Leitlinie für Web-Anwendungen/Web-Dienste

Für Web-Anwendungen/Web-Dienste sollte eine Leitlinie zur Verfügung stehen.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Leitlinie sollte insbesondere die Authentizität und Integrität der in Web-Anwendungen verwendeten Informationen abdecken.

12.2 Ordnungsgemäße Verarbeitung in Anwendungen

Ziel: Verhinderung von Fehlern, Verlust, unberechtigter Veränderung oder Missbrauch von Informationen in Anwendungen.

Es sollten angemessene Maßnahmen in Anwendungen, einschließlich der vom Benutzer entwickelten Anwendungen, eingeplant werden, die eine ordnungsgemäße Verarbeitung sicherstellen. Diese Maßnahmen sollten die Validierung von Eingabedaten, der internen Verarbeitung und der Ausgabedaten umfassen.

Zusätzliche Maßnahmen können für Systeme erforderlich sein, die sensible, wertvolle oder kritische Informationen verarbeiten oder Auswirkungen darauf haben. Diese Maßnahmen sollten auf der Grundlage von Sicherheitsanforderungen und einer Risikobewertung bestimmt werden.

12.2.1 Validierung von Eingabedaten

Die in ISO/IEC 27002:2005, 12.2.1, empfohlenen Maßnahmen gelten entsprechend.

12.2.2 Steuerung der internen Verarbeitung

Die in ISO/IEC 27002:2005, 12.2.2, empfohlenen Maßnahmen gelten entsprechend.

12.2.3 Integrität von Nachrichten

Die in ISO/IEC 27002:2005, 12.2.3, empfohlenen Maßnahmen gelten entsprechend.

12.2.4 Validierung von Ausgabedaten

Die in ISO/IEC 27002:2005, 12.2.4, empfohlenen Maßnahmen gelten entsprechend.

12.2.5 Entwicklung von Webanwendungen nach dem OWASP

Maßnahme

Bezüglich der Entwicklung von Webanwendungen sollte die Entwicklungsleitlinie des OWASP angewendet werden (siehe www.owasp.org).

Anleitung zur Umsetzung

Die Entwicklungsleitlinie des OWASP enthält ausführliche Ratschläge zu den folgenden Schlüsselbereichen bei der Entwicklung von Webanwendungen:

- Sicherheitsarchitektur;
- Authentisierung;
- Verwaltung von Sitzungen;
- Zugangskontrolle;
- Validierung von Eingabedaten;
- Ausgabecodierung/Escaping;
- Kryptografie;
- Fehlerbehandlung und Ereignisprotokollierung;
- Datenschutz;
- Kommunikationssicherheit;
- HTTP-Sicherheit;
- Sicherheitskonfiguration.

Für jede spezielle Webanwendung sollten die maßgeblichen Sicherheitsmaßnahmen umgesetzt werden.

Weitere Informationen

Die Entwicklungsleitlinie des OWASP erklärt, wie Webanwendungen anzulegen sind, damit sie die Anforderungen an die Verifizierungsstufen für Anwendungssicherheit, die in der Application Security Verification Standard (ASVS) des OWASP festgelegt sind, erfüllen oder übererfüllen. Die Verifizierungsstufen für Anwendungssicherheit konzentrieren sich auf die Analyse von Bauteilen, die die Anwenderebene des OSI-Modells darstellen. Die Leitlinie wurde mit folgenden Zielen entwickelt:

- Verwendung als Bezug;
- Verwendung, um Design-Entscheidungen zu treffen;
- Verwendung als Anleitung.

12.2.6 Code-Reviews

Maßnahme

Die Organisation sollte sicherstellen, dass Code-Reviews für geschäftskritische Anwendungen als Teil der Umsetzungs- und Änderungsprozesse durchgeführt werden.

Anleitung zur Umsetzung

Die Organisation sollte Code-Reviews entweder durch Anwendung von Werkzeugen für eine automatische statische Codeanalyse, durch manuelle Überprüfung oder beides durchführen.

Weitere Informationen

Ein Code-Review ist eine systematische Überprüfung des Quellcodes. Es wird damit beabsichtigt, Fehler zu erkennen und zu beheben, die in der anfänglichen Entwicklungsphase übersehen wurden, wodurch sich sowohl die Gesamtqualität der Software als auch die Fähigkeiten der Entwickler verbessern.

12.3 Kryptografische Maßnahmen

Ziel: Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen durch kryptografische Mittel.

Eine Leitlinie zum Einsatz kryptografischer Maßnahmen sollte entwickelt werden. Eine Verwaltung kryptografischer Schlüssel sollte zur Unterstützung der kryptografischen Techniken bereitstehen.

12.3.1 Leitlinie für die Anwendung kryptografischer Maßnahmen

Die in ISO/IEC 27002:2005, 12.3.1, empfohlenen Maßnahmen gelten entsprechend.

12.3.2 Verwaltung kryptografischer Schlüssel

Die in ISO/IEC 27002:2005, 12.3.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte ein zentrales Zertifikats-Managementsystem betreiben. Die Zertifikate sollten im Format X509v3 erstellt werden.

Wenn eine Organisation eine PKI betreibt, sollte es ein zentrales Zertifikats-Managementsystem geben. Folgende Dokumente sollten vorhanden sein:

Die folgenden Dokumente sollten für eine PKI vorhanden sein, die nicht ausschließlich technischen Zwecken dient:

- *Certificate Policy (CP);*
- *Erklärung zum Zertifizierungsbetrieb (CPS) (en: Certificate Practice Statement).*

Für jede PKI, die ausschließlich technischen Zwecken dient, müssen technische Dokumentationen vorhanden sein, die den Betrieb und die Sicherheitsnormen der PKI dokumentieren.

Für die Vergabe und den Entzug von Zertifikaten sollten verifizierbare Prozesse festgelegt sein.

Die Gültigkeit von Zertifikaten sollte dokumentiert werden.

12.4 Sicherheit von Systemdateien

Ziel: Sicherstellung der Sicherheit von Systemdateien.

Der Zugang zu Systemdateien und zum Programm Quellcode sollte gesteuert werden und IT-Projekte und unterstützende Aktivitäten sollten auf eine sichere Art und Weise durchgeführt werden. Es sollte sorgfältig vermieden werden, sensible Daten in Prüfumgebungen offen zu legen.

12.4.1 Steuerung von Software im Betrieb

Die in ISO/IEC 27002:2005, 12.4.1, empfohlenen Maßnahmen gelten entsprechend.

12.4.2 Schutz von Systemprüfdaten

Die in ISO/IEC 27002:2005, 12.4.2, empfohlenen Maßnahmen gelten entsprechend.

12.4.3 Zugangskontrolle zum Programm Quellcode

Die in ISO/IEC 27002:2005, 12.4.3, empfohlenen Maßnahmen gelten entsprechend.

12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Ziel: Erhalt der Sicherheit von Software und Informationen von Anwendungssystemen.

Projekt- und Supportumgebungen sollten streng überwacht werden.

Die verantwortlichen Manager für die Anwendungssysteme sollten auch für die Sicherheit der Projekt- oder Supportumgebungen verantwortlich sein. Sie sollten sicherstellen, dass alle vorgeschlagenen Systemänderungen daraufhin überprüft werden, dass sie weder die Sicherheit des Systems noch die der Betriebsumgebung kompromittieren.

12.5.1 Änderungskontrollverfahren

Die in ISO/IEC 27002:2005, 12.5.1, empfohlenen Maßnahmen gelten entsprechend.

12.5.2 Technische Überprüfung von Anwendungen nach Änderungen am Betriebssystem

Die in ISO/IEC 27002:2005, 12.5.2, empfohlenen Maßnahmen gelten entsprechend.

12.5.3 Einschränkung von Änderungen an Softwarepaketen

Die in ISO/IEC 27002:2005, 12.5.3, empfohlenen Maßnahmen gelten entsprechend.

12.5.4 Informationsleck

Die in ISO/IEC 27002:2005, 12.5.4, empfohlenen Maßnahmen gelten entsprechend.

12.5.5 Ausgelagerte Softwareentwicklung

Die in ISO/IEC 27002:2005, 12.5.5, empfohlenen Maßnahmen gelten entsprechend.

12.6 Verwaltung technischer Schwachstellen

Ziel: Verringerung von Risiken, die durch die Ausnutzung veröffentlichter technischer Schwachstellen entstehen.

Die Verwaltung technischer Schwachstellen sollte auf eine wirksame, systematische und wiederholbare Art umgesetzt werden, wobei Messungen vorzunehmen sind, die die Wirksamkeit nachweisen. Diese Betrachtungen sollten Betriebssysteme und alle weiteren genutzten Anwendungen einschließen.

12.6.1 Steuerung technischer Schwachstellen

Die in ISO/IEC 27002:2005, 12.6.1, empfohlenen Maßnahmen gelten entsprechend.

12.6.2 Penetrationsprüfungen von Anwendungen

Maßnahme

Die Organisation sollte regelmäßige Penetrationsprüfungen von Anwendungen durchführen (Webanwendungen, Client-Server-Anwendungen, Datenbanken usw.).

Anleitung zur Umsetzung

Regelmäßige Penetrationsprüfungen von Anwendungen sollten bei geschäftskritischen Anwendungen jedes Jahr festgelegt sein. Außerdem sollten Penetrationsprüfungen nach jeder wesentlichen Aktualisierung oder Änderung einer Anwendung erfolgen (z. B. wenn der Umgebung eine neue Anwendung hinzugefügt wurde, wenn eine wesentliche Funktion in eine Anwendung eingefügt wurde usw.).

Die Häufigkeit und der Grad der Prüfungen sollten dem Grad entsprechen, in dem die Anwendungen organisationsübergreifend eingesetzt sind. Im Allgemeinen dürfen automatische Sicherheitsscanner verwendet werden, aber die Scan-Ergebnisse müssen durch eine manuelle Überprüfung eingefügt werden (um falsch-positive und falsch-negative Ergebnisse zu entfernen) sowie über genaue Prüfungen auf der Grundlage einer formellen methodischen Vorgehensweise.

Die Arbeitsgruppe, die die Penetrationsprüfungen durchführt, darf aus externen oder organisationsinternen Personen zusammengesetzt sein. Ihre Mitglieder sollten über nachgewiesene Erfahrungen auf dem Gebiet der vorausschauenden Sicherheit verfügen und sollten regelmäßige Sicherheitsschulungen besuchen, um umsetzbare Ergebnisse sicherzustellen.

Weitere Informationen

Eine Penetrationsprüfung ist ein vorausschauender Sicherheitsdienst, der die Ausführung vollständiger ethischer Hacking-Prüfungen umfasst. Sie beruht auf inferentiellen Angriffstechniken, die dazu dienen, Schwachstellen zu identifizieren, die allein mittels automatischer Sicherheitsscanner nicht entdeckt werden können. Sofern die Penetrationsprüfungen von Anwendungen ordnungsgemäß durchgeführt werden, führen sie zu einer objektiven und wiederholbaren Beurteilung der Sicherheitslage von Anwendungen. Somit können sie Sicherheitsschwachstellen bezüglich der Konstruktion, Umsetzung und Konfiguration aufdecken.

12.6.3 Penetrationsprüfungen von Infrastrukturen

Maßnahme

Die Organisation sollte regelmäßige Penetrationsprüfungen von kritischen Infrastrukturen durchführen (Server, Workstations, Netzwerkausstattung usw.).

Anleitung zur Umsetzung

Regelmäßige Penetrationsprüfungen sollten jedes Jahr durchgeführt werden. Außerdem sollten Penetrationsprüfungen nach jeder wesentlichen Aktualisierung oder Änderung der Infrastruktur erfolgen (z. B. Aktualisierung des Betriebssystems, wenn ein neues Subnetz in die Netzwerkumgebung eingefügt wurde usw.).

Der Grad der Prüfungen sollte dem Grad entsprechen, in dem das System und das Netz organisationsübergreifend eingesetzt sind. Im Allgemeinen dürfen automatische Sicherheitsscanner verwendet werden, aber die Scan-Ergebnisse müssen durch eine manuelle Überprüfung eingefügt werden (um falsch-positive und falsch-negative Ergebnisse zu entfernen) sowie über genaue Prüfungen auf der Grundlage einer formellen methodischen Vorgehensweise.

Anschlussstellen nach außen sollten regelmäßig nach aktuellen Normen auf Sicherheitsschwachstellen geprüft werden.

Die Arbeitsgruppe, die die Penetrationsprüfungen durchführt, darf aus externen oder organisationsinternen Personen zusammengesetzt sein. Ihre Mitglieder sollten über nachgewiesene Erfahrungen auf dem Gebiet der vorausschauenden Sicherheit verfügen und sollten regelmäßige Sicherheitsschulungen besuchen, um umsetzbare Ergebnisse sicherzustellen.

Weitere Informationen

Eine Penetrationsprüfung ist ein vorausschauender Sicherheitsdienst, der die Ausführung vollständiger ethischer Hacking-Prüfungen umfasst. Sie beruht auf inferentiellen Angriffstechniken, die dazu dienen, Schwachstellen zu identifizieren, die allein mittels automatischer Sicherheitsscanner nicht entdeckt werden können. Sofern die Penetrationsprüfungen von Infrastrukturen ordnungsgemäß durchgeführt werden, führen sie zu einer objektiven und wiederholbaren Beurteilung der Sicherheitslage von Systemen und Netzen im Allgemeinen. Eine der verbreitetsten methodischen Vorgehensweisen für Penetrationsprüfungen ist das Open Source Security Testing Methodology Manual (siehe www.osstmm.org).

13 Behandlung von Informationssicherheitsvorfällen

13.1 Melden von Informationssicherheitsereignissen und Schwachstellen

Ziel: Sicherstellung, dass Informationssicherheitsereignisse und Schwachstellen in Verbindung mit Informationssystemen so kommuniziert werden, dass rechtzeitig Korrekturmaßnahmen ergriffen werden können.

Formale Verfahren für das Melden von Ereignissen und für die Eskalation sollten festgelegt sein. Die Meldeverfahren für die verschiedenen Arten von Ereignissen und Schwachstellen, die einen Einfluss auf die Sicherheit organisationseigener Werte haben könnten, sollten allen Mitarbeitern, Vertragsnehmern und Drittbenutzern bewusst gemacht werden. Sie sollten verpflichtet sein, alle Informationssicherheitsereignisse und Schwachstellen so schnell wie möglich an die ausgewiesene Anlaufstelle zu melden.

13.1.1 Melden von Informationssicherheitsereignissen

Die in ISO/IEC 27002:2005, 13.1.1, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte eine Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle einrichten, die entsprechend ausgebildet ist und über die Fertigkeiten verfügt, umgehend auf Sicherheitsvorfälle zu reagieren und die notwendigen Maßnahmen umzusetzen. Wenn ein Geschäftsprozess organisationsübergreifend betrieben wird, so sollten die einzelnen eingesetzten Arbeitsgruppen zur Reaktion auf Sicherheitsvorfälle – entsprechend den Anforderungen und der Risikobewertung für diesen Geschäftsprozess – aufeinander abgestimmt werden, oder es sollte gegebenenfalls eine gemeinsame Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle von den beteiligten Organisationen eingesetzt werden. Die Organisation sollte dazu einen Verantwortlichen für Fragen zum Umgang mit Sicherheitsvorfällen und die Kontakte für die operative Durchführung des Managements von Sicherheitsvorfällen benennen.

Die Organisation sollte darüber hinaus an vorhandenen organisationsübergreifenden Managementsystemen für Sicherheitsvorfälle teilnehmen, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden.

Eine angemessene Reaktionszeit der Arbeitsgruppe sollte sichergestellt sein.

13.1.2 Melden von Sicherheitsschwachstellen

Die in ISO/IEC 27002:2005, 13.1.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte erkannte Sicherheitsschwachstellen bei Geschäftsprozessen, die mehrere Organisationen betreffen, umgehend an die anderen beteiligten Organisationen melden.

Die Organisation sollte in bereits vorhandenen übergreifenden Gremien und Foren, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, mitarbeiten, um Informationen über Sicherheitsschwachstellen untereinander – soweit notwendig und für Dritte interessant – auszutauschen.

13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

Ziel: Sicherstellung, dass ein einheitlicher und wirksamer Ansatz für den Umgang mit Informationssicherheitsvorfällen angewendet wird.

Verantwortlichkeiten und Verfahren sollten etabliert sein, um Informationssicherheitsereignisse und Schwachstellen wirksam zu behandeln, sobald sie gemeldet wurden. Ein Prozess der ständigen Verbesserung sollte auf die Reaktion, Überwachung, Beurteilung und den gesamten Umgang mit Informationssicherheitsvorfällen angewendet werden.

Wenn Beweise erforderlich sind, sollten diese gesammelt werden, um die Einhaltung gesetzlicher Anforderungen sicherzustellen.

13.2.1 Verantwortlichkeiten und Verfahren

Die in ISO/IEC 27002:2005, 13.2.1, empfohlenen Maßnahmen gelten entsprechend.

13.2.2 Aus Informationssicherheitsvorfällen lernen

Die in ISO/IEC 27002:2005, 13.2.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte in bereits vorhandenen Organisationen mitarbeiten, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, um insbesondere für allgemeine Geschäftsprozesse gemeinsam aus Sicherheitsvorfällen zu lernen und entsprechende Maßnahmen abzuleiten.

13.2.3 Sammeln von Beweisen

Die in ISO/IEC 27002:2005, 13.2.3, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte mit Organisationen, die Informationen sammeln und gemeinsam nutzen zusammenarbeiten, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden.

14 Betriebskontinuitätsmanagement

14.1 Informationssicherheitsaspekte hinsichtlich des Betriebskontinuitätsmanagements

Ziel: Unterbrechungen von Geschäftstätigkeiten entgegenzuwirken, und um kritische Geschäftsprozesse vor den Auswirkungen größerer Ausfälle von Informationssystemen oder vor Katastrophen zu schützen und ihre rechtzeitige Wiederaufnahme sicherzustellen.

Ein Prozess im Rahmen des Betriebskontinuitätsmanagements sollte umgesetzt werden, um die Auswirkungen auf die Organisation gering zu halten und sich vom Verlust von Informationswerten (die z. B. Folge von Naturkatastrophen, Unfällen, Geräteausfällen und mutwilligen Beschädigungen sein können) durch eine Kombination vorbeugender und wiederherstellender Maßnahmen bis auf ein annehmbares Niveau zu erholen.

Dieser Prozess sollte die kritischen Geschäftsprozesse identifizieren und die Anforderungen an das Informationssicherheitsmanagement bezüglich der Weiterführung des Geschäftsbetriebs in andere Kontinuitätsanforderungen einbeziehen, die sich auf solche Aspekte wie Betrieb, Personal, Werkstoffe, Transport und Einrichtungen beziehen.

Die Folgen von Katastrophen, Sicherheitsausfällen, des Verlustes von Diensten und der Verfügbarkeit von Diensten sollten Gegenstand einer Analyse der Auswirkungen auf den Geschäftsbetrieb sein. Betriebskontinuitätspläne sollten entwickelt und umgesetzt werden, um sicherzustellen, dass wesentliche Geschäftsprozesse in der erforderlichen Zeit wiederhergestellt werden können. Informationssicherheit sollte ein fester Bestandteil des gesamten Prozesses der Betriebskontinuität sowie weiterer Managementprozesse innerhalb der Organisation sein.

Das Betriebskontinuitätsmanagement sollte zusätzlich zum allgemeinen Risikobewertungsprozess auch Maßnahmen zur Identifizierung und Verringerung von Risiken umfassen, und die Folgen von schädigenden Vorfällen begrenzen, sowie sicherstellen, dass die für Geschäftsprozesse nötigen Informationen greifbar sind.

14.1.1 Einbeziehen von Informationssicherheit in den Prozess des Betriebskontinuitätsmanagements

Die in ISO/IEC 27002:2005, 14.1.1, empfohlenen Maßnahmen gelten entsprechend.

14.1.2 Betriebskontinuität und Risikobewertung

Die in ISO/IEC 27002:2005, 14.1.2, empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Umsetzungsvorgaben

Die an einem gemeinsamen Geschäftsprozess beteiligten Organisationen sollten für den gesamten Vorgang eine Geschäftsauswirkungsanalyse durchführen.

Weitere luftverkehrsspezifische Informationen

Die Geschäftsauswirkungsanalyse sollte folgende Schritte nach ISO/IEC 27031:2011 enthalten:

- *Auswahl der einzubeziehenden Organisationseinheiten und (Einzel-)Prozesse;*
- *Kritikalitätsanalyse für die betreffenden Werte (Assets);*
- *Festlegung von Kritikalitätskategorien und Schadensszenarien;*
- *Festlegung der zu betrachtenden Bewertungszeiträume;*
- *besondere Termine und Ereignisse;*
- *Kritikalitätsanalyse*
- *Priorisierung der einzelnen Prozesse*