Informationssicherheitsrichtlinie für Betreiber und Entwickler von IT-Systemen (ISEC-Richtlinie BE)

- Lizenzfrei –

(Diese Richtlinie enthält lediglich die Überschriften der geforderten Controls ohne Umsetzungsmaßnahmen. Die vollständige Richtlinie erhalten Sie, wenn Sie eine gültige Lizenz für die DIN EN ISO/IEC 27001/2 Normreihe besitzen)

Dokumentennummer: ITAI-RL-002.002.001

Gliederung

0 Einleitung

Die vorliegende Informationssicherheitsrichtlinie (ISEC-Richtlinie) des FMG-Konzerns für Betreiber und Entwickler von IT-Systemen (ISEC-Richtlinie BE) basiert auf dem Informationssicherheits-Standard des Bundesverbandes der deutschen Luftverkehrswirtschaft (BDL), Arbeitsgruppe Informationssicherheit (Code of Practice in Practice V3.2. (CoPiP)), sowie der darin referenzierten aktuellsten ISO 27xxx Standards.

Die Schreibweisen der Informationssicherheits-Begriffe in diesem Dokument orientieren sich an der Schreibweise der Standards ISO 27001 und ISO 27002 und können daher von der bekannten und üblicherweise verwendeten Schreibweise im FMG-Konzern abweichen.

1 Anwendungsbereich

1.1 Zielsetzung

Die ISEC-Richtlinie BE des FMG-Konzerns definiert verbindliche Sicherheits-Mindestvorgaben für die Entwicklung, die Einführung, den Betrieb, die Außerbetriebnahme und die Entsorgung von informationsverarbeitenden Systemen im FMG-Konzern.

Bei kritischen Geschäftsprozessen sind gegebenenfalls zusätzliche Maßnahmen zu ergreifen.

Die ISEC-Richtlinie BE ist Bestandteil des FMG-Konzern-Informationssicherheitsrahmenwerks (ISEC-Framework), aus dessen Vorgaben Sicherheitskonzepte und -maßnahmen so abgeleitet werden, dass stets ein angemessener Schutz gewährleistet ist.

Die ISEC-Richtlinie BE beschreibt nicht die Umsetzung der Sicherheits-Mindestvorgaben. Diese muss jeweils projekt- bzw. bereichsspezifisch erarbeitet werden.

1.2 Geltungsbereich und Gültigkeit

Die ISEC-Richtlinie BE gilt verbindlich und ortsunabhängig für alle Bereiche und Beteiligungsgesellschaften des FMG-Konzerns und für Auftraggeber sowie Auftragnehmer, die direkt oder indirekt bei der Entwicklung, der Einführung, dem Betrieb sowie der Außerbetriebnahme und Entsorgung von Anwendungen und informationsverarbeitenden Systemen im FMG-Konzern beteiligt sind.

Als Entwicklung ist die systematische Herstellung von Computerprogrammen (Software) definiert. Im Gegensatz zur reinen Programmierung beinhaltet die Entwicklung den gesamten Softwareentwicklungsprozess. Neben der eigentlichen Programmierarbeit gehört dazu auch das Erarbeiten der Anforderungen an die Software sowie das Erstellen einer sicheren Softwarearchitektur und die Planung der Umsetzung.

Die ISEC-Richtlinie BE gilt somit auch für die Neuentwicklung und Änderung von Software-Anwendungen und informationsverarbeitenden Systemen, die im Auftrag des FMG-Konzerns sowie dessen Beteiligungsgesellschaften entwickelt werden. Dies gilt analog auch für die Anpassung von Standard-Softwareprodukten.

Die vorliegende ISEC-Richtlinie BE tritt mit Wirkung zum 19.07.2023 in Kraft und ist verbindlich für alle ab diesem Zeitpunkt neu eingeführten IT-Systeme/Anwendungen einzuhalten.

Für zum Stichtag bereits im Einsatz bzw. in Realisierung befindliche IT-Systeme/Anwendungen sind die Vorgaben nicht verpflichtend, sollten aber soweit wie möglich berücksichtigt werden.

1.3 Rollen und Verantwortlichkeiten

1.3.1 FMG-Informationssicherheitsbeauftragter

Die ISEC-Richtlinie BE wird vom FMG-Konzern ISEC-Beauftragten erarbeitet und in Kraft gesetzt. Er wird im Intranet des FMG-Konzerns veröffentlicht. Die ISEC-Richtlinie BE wird jährlich oder bei Bedarf überprüft und den aktuellen organisatorischen Bedingungen, neuen IT-Entwicklungen und Bedrohungen der Informationssicherheit angepasst.

Die Rollen des ISEC-Managements des FMG-Konzerns sind in der Informationssicherheitsleitlinie (ISEC-Leitlinie) beschrieben. Eine wichtige Rolle hier ist die Rolle Information Security Assurance.

1.3.2 Information Security Assurance

Zur ISEC-Richtlinie BE können durch Information Security Assurance noch zusätzliche technische Vorgaben erstellt werden. Die security-relevanten Logfiles werden durch Information Security Assurance analysiert.

1.3.3 Auftraggeber und Betreiber

Zusätzliche Rollen innerhalb der ISEC-Richtlinie BE sind die des Auftraggebers und des Betreibers. Mit dem Begriff „Betreiber" sind alle Betreiber (operativer Betrieb) von Informationssystemen gemeint. Mit dem Begriff „Auftraggeber" ist der für ein System Verantwortliche gemeint. Im Sinne der ISEC-Richtlinie BE ist dies der Unternehmensteil, der das System in Auftrag gegeben hat, selbst betreibt oder durch einen Dritten betreiben lässt.

Der Auftraggeber hat dafür zu sorgen, dass die Einhaltung der ISEC-Richtlinie BE durch ihn oder die von ihm beauftragten Betreiber sichergestellt ist. Das beinhaltet, dass die vom Betreiber zu gewährleistenden ISEC-Regelungen vertraglich klar fixiert sind.

Innerhalb des betreffenden Unternehmensteils (Auftraggeber) tragen die personalverantwortlichen Führungskräfte die Verantwortung für die Einhaltung der ISEC-Richtlinie BE.

1.3.4 Informationsverantwortlicher

Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich (siehe hierzu: IT-Nutzungsrichtlinie). Typischerweise gehört er der ersten oder zweiten Führungsebene an oder hat bereichsübergreifende Aufgaben (z.B. Revision, Beihilfe, ISEC-Beauftragter, Arbeitsschutz, Datenschutz). Bei Aufgaben- und Funktionsänderungen passt er die Berechtigungen entsprechend an. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch ihn auch an andere Mitarbeiter delegiert werden.

1.3.5 Projekt-/Produktverantwortlichen

Der Projekt-/Produktverantwortliche ist verantwortlich für die Umsetzung der Vorgaben der ISEC-Richtlinie BE bei der Entwicklung, Einführung, Änderung sowie Aussonderung und Entsorgung von IT-Systemen sowie Anwendungen/Software.

1.4 Ausnahmeregelung

Abweichungen von der ISEC-Richtlinie BE sind durch den Auftraggeber bzw. durch den Betreiber oder Projekt-/Produktverantwortlichen, soweit vertraglich in seiner Verantwortung, beim FMG-Konzern-ISEC-Beauftragten mit Angabe von Gründen schriftlich mit dem bereitgestellten Formular zu melden.

Können einzelne Regeln der ISEC-Richtlinie BE nachweislich technisch nicht realisiert werden (z.B. Virenschutz auf Switches), so kann auf diese Meldungen verzichtet werden.

1.5 Überwachung

Die Umsetzung der ISEC-Richtlinie BE wird stichprobenartig in Form von Audits durch den ISEC-Beauftragten des FMG-Konzerns überprüft.

2 Referenzen

Die folgenden Empfehlungen und internationalen Standards enthalten Bestimmungen, die – soweit auf sie im vorliegenden Standard referenziert wird – anwendbare Bestimmungen dieses Standards sind.

- 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 management.
- ISO/IEC 27005:2018
- CoPiP 3.2, Version 2019
- Anforderungskatalog Cloud Computing (C5), Version 2020

3 Begriffe & Abkürzungen

Hier wird auf das eigenständige Dokument **„Begriffe & Abkürzungen des FMG-Konzerns zur Informationssicherheit“** verwiesen sowie auf ISO/IEC 27000.

4 Informationssicherheitsmanagement in der Luftfahrt

4.1 Struktur dieses Standards und Anwendungen dieses Standards

Dieser Standard ist gemäß der CoPiP Version 3.2 sowie der ISO/IEC 27002 aufgebaut.

- Maßnahmen aus dem CoPiP Version 3.2 bzw. der ISO/IEC 27002, soweit sie für diesen Standard zutreffen, sind im vorliegenden Standard schwarz markiert und müssen durch geeignete Verfahren erfüllt werden.
- Ergänzende Maßnahmen/Anforderungen zu den in der ISO/IEC 27002 genannten Maßnahmen, die spezifisch für den FMG Konzern gelten, sind im vorliegenden Standard blau markiert und sind als Mindestanforderungen einzuhalten.
- Ergänzende luftfahrtspezifische Maßnahmen gemäß CoPiP 3.2 (BDL), sind im vorliegenden Standard grün markiert und müssen für KRITIS-relevante Systeme als Mindestanforderungen eingehalten werden, selbst wenn die Anforderung als „sollte“ definiert ist.Analyse & Bewertung von Informationssicherheitsrisiken (ISEC-Risiken)

4.2.1 Einführung Informationssicherheitsrisikomanagement (ISEC-Risikomanagement)

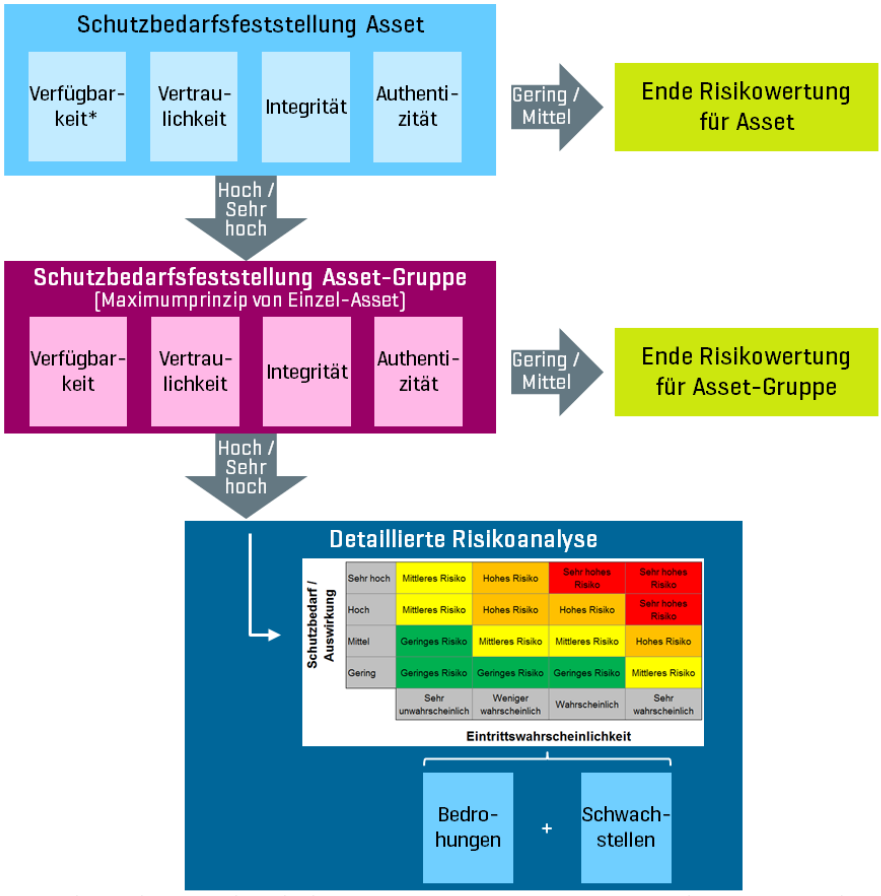
Die in ISO/IEC 27002 Kapitel 4 aufgeführten Maßnahmenziele und Inhalte müssen entsprechend angewendet werden. Das ISEC-Risikomanagement sollte gemäß ISO/IEC 27005 erfolgen.

Beim ISEC-Risikomanagement sollten alle Werte (Informationen, Anwendungen, Systeme) berücksichtigt werden.

4.2.2 Anwendung ISEC-Risikomanagement

Grundlegende Vorgehensweise

Das ISEC-Risikomanagement beim FMG-Konzern wird entsprechend der nachstehenden Vorgehensweise durchgeführt:



*) einschließlich maximal hinnehmbare Zeitspanne für Datenverlust (RPO) und maximal tolerierbare Ausfallzeit

Die Dokumentation erfolgt mit Hilfe des aktuell beim FMG-Konzern freigegebenen und veröffentlichten Tools für ISEC-Risikomanagement.

Im Rahmen der Risikobewertung werden folgende Aktivitäten durchgeführt:

Schritt 1: Schutzbedarfsfeststellung Asset

Für ein ausgewähltes Asset wird der Schutzbedarf anhand der Informationssicherheitsaspekte mit vordefinierten Abstufungen bestimmt. Diese Aspekte sind:

a) **Verfügbarkeit**: Sicherstellung, dass Daten und Systeme präsent und innerhalb einer definierten Zeit nutzbar sind.
   Die **maximal tolerierbare Ausfallzeit (MTA)** gibt den Zeitraum an, innerhalb dessen bei einem Ausfall die betroffenen Systeme wieder in einem funktionsfähigen Zustand sein müssen.
   Mit der Definition der **maximal hinnehmbaren Zeitspanne für Datenverlust (RPO)** wird festgelegt, für welchen zurückliegenden Zeitraum Daten bei einem Ausfall unwiederbringlich verloren sein dürfen, d.h. in welchem Intervall Backups der Daten erfolgen müssen.
b) **Vertraulichkeit**: Sicherstellung, dass Systeme und Daten nur für berechtigte Personen zugänglich/einsehbar sind.
c) **Integrität**: Sicherstellung, dass Systeme und Daten vollständig und richtig zur Verfügung stehen.
d) **Authentizität**: Sicherstellung, dass die Datenherkunft nachgewiesen werden kann und die Glaubwürdigkeit der Daten gesichert ist.

Der Gesamt-Schutzbedarf des Wertes wird dabei vom höchsten Wert eines Aspektes bestimmt (Maximumprinzip).

Die Einstufung erfolgt anhand folgender Kriterien:

Aspekt	Gering	Mittel	Hoch	Sehr hoch
Verfügbarkeit	Gering	Mittel	Hoch	Sehr hoch
Vertraulichkeit	Offen	Dienstlich	Vertraulich	Streng vertraulich
Integrität	n/a	Normal	Hoch	n/a
Authentizität	n/a	Normal	Hoch	n/a

Sofern als maximaler Wert für den Schutzbedarf Gering oder Mittel ermittelt wurde, kann auf eine weitergehende Schutzbedarfsfeststellung des Wertes bzw. im nächsten Schritt auf eine detaillierte Risikoanalyse verzichtet werden.

Schritt 2: Schutzbedarfsfeststellung Asset-Gruppe

Dieser Schritt soll dabei helfen, Werte mit identischem Schutzbedarf bzw. vergleichbaren Bedrohungen als Asset-Gruppe zusammenzufassen. Der Schutzbedarf für die Asset-Gruppe ergibt sich aus dem jeweils höchsten Wert eines darin enthaltenen Wertes (Maximumprinzip). Die Gruppierung kann auch dazu führen, dass der Schutzbedarf für die Asset-Gruppe höher ist als für die einzelnen Werte.

Für die Einstufung der unterschiedlichen Aspekte kommen dieselben Werte wie bei
Schritt 1 (siehe vorstehende Tabelle) zum Einsatz.

Sofern für eine Asset-Gruppe ein Schutzbedarf Gering oder Mittel festgestellt wurde, kann auf eine detaillierte Risikoanalyse für diese Asset-Gruppe verzichtet werden. Sofern der Gesamt-Schutzbedarf jedoch bei Hoch oder Sehr hoch liegt, muss eine detaillierte Risikoanalyse gemäß Schritt 3 erfolgen.

Schritt 3: Identifikation Umsetzung erforderliche Sicherheitsmaßnahmen

Die vorgeschriebenen – insbesondere in der vorliegenden Richtlinie aufgestellten – Sicherheitsmaßnahmen stellen grundsätzlich ein ausreichendes Sicherheitsniveau zur Gewährleistung des jeweiligen Schutzbedarfs dar. Aus diesem Grund ist in diesem Schritt festzustellen, inwieweit die Vorgaben umgesetzt sind bzw. eingehalten werden und wo ggf. noch Handlungsbedarf besteht.

Dabei können folgende Konstellationen als ausreichend im Sinne eines angemessenen Schutzes hinsichtlich Informationssicherheit betrachtet werden:

- Für das Asset/die Asset-Gruppe wurden alle Sicherheitsmaßnahmen gemäß den aktuellen Vorgaben unter Berücksichtigung des Schutzbedarfs umgesetzt bzw. werden eingehalten.
- Für nicht umgesetzte Sicherheitsmaßnahmen gemäß den aktuellen Vorgaben existiert eine gültige Ausnahmegenehmigung.

Sofern keine der beiden Konstellationen zutrifft, muss für das betreffende Asset/die Asset-Gruppe eine detaillierte Risikoanalyse durchgeführt werden, um eine Identifikation der bestehenden Risiken zu gewährleisten.

Schritt 4: Detaillierte Risikoanalyse

Der in Schritt 1 bzw. 2 ermittelte Schutzbedarf entspricht dem potenziellen Schaden und damit der Y-Achse der Informationssicherheitsrisikomatrix. Im Rahmen der detaillierten Risikoanalyse muss der Wert der X-Achse, der sogenannten Eintrittswahrscheinlichkeit, einer Kombination aus Bedrohung und Schwachstelle möglicher Szenarien bestimmt werden.

Dabei werden zunächst die für das betreffende Asset relevanten Bedrohungen aus folgenden Kategorien ausgewählt:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

Die Bedrohungen sind anhand der allgemeinen Gegebenheiten (wie häufig/verbreitet ist sie) und der FMG-Konzern-spezifischen Exponiertheit (besonderes „Ziel" aufgrund z.B. geografischer Gegebenheiten, Geschäftstätigkeit etc.) mit einer Wahrscheinlichkeit zu bestimmen.

Zu den Bedrohungen gilt es, jeweils eine oder mehrere Schwachstellen, also mögliche konkrete Verwundbarkeiten, zu identifizieren und unter Berücksichtigung existierender oder eben nicht existierender Sicherheitsmaßnahmen mit einem Wert für die Ausnutzbarkeit zu versehen.

Aus der Kombination der Bedrohung und Schwachstelle ergibt sich gemäß nachfolgender Matrix die potenzielle Eintrittswahrscheinlichkeit:

Ausnutzbarkeit Schwachstelle	Nicht vorhanden	Sehr selten	Selten	Häufig/regelmäßig	Permanent
Sehr leicht	sehr unwahrscheinlich	weniger wahrscheinlich	wahrscheinlich	sehr wahrscheinlich	sehr wahrscheinlich
Leicht	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich	wahrscheinlich	sehr wahrscheinlich
Schwierig	sehr unwahrscheinlich	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich	wahrscheinlich
Sehr schwierig	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich
Nicht vorhanden	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich

Wahrscheinlichkeit Bedrohung

In Kombination mit dem ermittelten Schutzbedarf ergibt die Eintrittswahrscheinlichkeit das festgestellte ISEC-Risiko entsprechend der nachstehenden Informationssicherheitsrisikomatrix:

Schutzbedarf / Auswirkung				
Sehr hoch	Mittleres Risiko	Hohes Risiko	Sehr hohes Risiko	Sehr hohes Risiko
Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko	Sehr hohes Risiko
Mittel	Geringes Risiko	Mittleres Risiko	Mittleres Risiko	Hohes Risiko
Gering	Geringes Risiko	Geringes Risiko	Geringes Risiko	Mittleres Risiko
	Sehr unwahrscheinlich	Weniger wahrscheinlich	Wahrscheinlich	Sehr wahrscheinlich

Eintrittswahrscheinlichkeit

Risiken der Stufe Hohes Risiko bzw. Sehr hohes Risiko müssen – soweit möglich und wirtschaftlich sinnvoll – entweder mit entsprechenden Maßnahmen behandelt werden (Reduzierung, Transfer, Vermeidung) oder von einer hierfür zuständigen Stelle im Management bewusst akzeptiert werden. Dies ist in entsprechender Weise und für Dritte nachvollziehbar zu dokumentieren, ebenso wie das (voraussichtlich) verbleibende Restrisiko nach Umsetzung der vorgesehenen Risikobehandlungs-Maßnahmen.

4.2.3 Risikobehandlung

Für die analysierten Risiken sind die entsprechenden Maßnahmen durch die beteiligten Verantwortlichen einvernehmlich festzulegen und zu dokumentieren.

4.3 Auswahl von Maßnahmen

Gemäß den Ergebnissen der ISEC-Risikoanalyse müssen die in Kapitel 4.1 näher erläuterten Maßnahmen ausgewählt und umgesetzt werden.

4.4 Umgang mit und Dokumentation von Ausnahmen

Bei folgenden besonderen Umständen können Ausnahmen gemacht werden:

Es sind Ersatzmaßnahmen (Maßnahmen, die nicht unter 4.3 aufgeführt sind) realisiert, die zumindest die gleiche Effizienz und den gleichen Schutzwert aufweisen.

Aufgrund von objektbezogenen Risikobewertungen wird nachgewiesen, dass Ersatzmaßnahmen mit einem geringeren Schutzwert bzw. der Wegfall einer Maßnahme akzeptiert werden können.

Die Ausnahmen sind umfassend zu dokumentieren. Der Verantwortliche muss die Abweichungen anhand einer Risikoanalyse bewerten und die Ergebnisse dem ISM schriftlich mitteilen.

4.5 Levels of Trust

Da die Leistungserbringung im Luftverkehr stark von der Zusammenarbeit der einzelnen Teilnehmer geprägt ist, hängt das ISM einer Organisation wesentlich vom ISM der Organisationen ab, mit denen man in der Leistungserbringung zusammenarbeitet.

Die Gewährleistung der Sicherheit der Informationen und der informationsverarbeitenden Systeme einzelner Organisationen im gemeinsamen Geschäftsprozess sowie der dahinter stehenden eigenen Geschäftsprozesse ist mit einem hohen Aufwand an individuellen Vereinbarungen und Überprüfungen verbunden.

Gemäß CoPiP 3.2 wurde vereinbart, dass überprüfte Vertrauensstellungen (aus der 1:1-Beziehung zweier Organisationen oder durch die Überprüfung durch Externe) in weiteren gemeinsamen Geschäftsprozessen (auch mit dritten Organisationen) anerkannt werden.

Die Vertrauensstufe bzw. „Level-of-Trust der Organisation" (abgekürzt LoT) bezieht sich grundsätzlich auf die jeweilige Organisation. Die Einstufung bezieht sich dabei immer auf den Teil des Kernflugprozesses, der der jeweiligen Organisation erbracht wird. Hierbei sind v.a. potentielle ISEC-Risiken, die durch Koppelung der Geschäftsprozesse für die jeweiligen Organisationen entstehen können, zu berücksichtigen.

Die Einstufung gemäß LoT der einzelnen im Folgenden näher beschriebenen Controls für den FMG-Konzern inklusive Einbeziehung des Schutzbedarfs hinsichtlich Vertraulichkeit und Verfügbarkeit findet sich in der Übersichtstabelle im Anhang 2.

Nach der in diesem Kapitel beschriebenen Risikobewertung werden die umzusetzenden technischen und organisatorischen Maßnahmen gemäß der unten stehenden Kriterien identifiziert:

- IT-Abhängigkeit ist vorhanden. Es existieren keine technischen Redundanzen bzw. keine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT1 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)

- IT-Abhängigkeit ist vorhanden. Es existieren technische Redundanzen, aber keine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT2 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)

- IT-Abhängigkeit ist vorhanden. Es existieren zudem technische Redundanzen und eine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT3 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)

- Es ist keine IT-Abhängigkeit vorhanden:
  ⇨ Keine Vorgabe konkreter Maßnahmen

Dabei muss beachtet werden, dass die Möglichkeit der Risikoakzeptanz oder Übertragbarkeit gem. CoPiP nur unter der Voraussetzung von §8a BSIG (Verhältnis Aufwand zu Folgen eines Ausfalls/einer Beeinträchtigung) erfolgen kann.

5 Sicherheitsleitlinie

5.1 Informationssicherheitsleitlinie

Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.

5.1.1 Vorgaben der Leitung für Informationssicherheit

Maßnahme: Ein Satz Informationssicherheitsrichtlinien sollte festgelegt sein, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.

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 Informationssicherheitsrichtlinien

Maßnahme: Die Informationssicherheitsrichtlinien sollten in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

BSIG-66: Richtlinien müssen regelmäßig (d.h. zumindest jährlich) auf Angemessenheit und Wirksamkeit hin überprüft werden.

5.2 Führung

a) Das Management sollte den Bedarf an Beratung durch interne oder externe Fachleute für Informationssicherheit identifizieren und die Ergebnisse daraus überprüfen und organisationsweit die sich daraus ergebenden Aktivitäten koordinieren.
b) Je nach Größe der Organisation kann diese Verantwortung von einem eigenen Managementforum oder einem bereits vorhandenen Managementgremium, wie dem Vorstand, wahrgenommen werden.

5.2.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Informationssicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie:

a) sicherstellt, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbart sind;
b) sicherstellt, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden;
c) sicherstellt, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
d) die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Informationssicherheitsmanagementsystems vermittelt;
e) sicherstellt, dass das Informationssicherheitsmanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt
f) Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Informationssicherheitsmanagementsystems beitragen können;
g) fortlaufende Verbesserungen fördert und
h) andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

5.2.2 Politik

Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die:

a) Für den Zweck der Organisation angemessen ist;
b) Informationssicherheitsziele (siehe ISO 27001, Kap. 6.2.) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;
c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält und

d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

5.2.3 Managementbewertung

Die oberste Leitung muss das Informationssicherheitsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.
Die Managementbewertung muss folgende Aspekte behandeln:
a) den Status von Maßnahmen vorheriger Managementbewertungen;
b) Veränderungen bei externen und internen Themen, die das Informationssicherheitsmanagementsystem betreffen;
c) Rückmeldungen über die Informationssicherheitsleistungen, einschließlich Entwicklungen bei:
    1) Nichtkonformität und Korrekturmaßnahmen;
    2) Ergebnissen von Überwachungen und Messungen;
    3) Auditierergebnissen und
    4) Erreichung von Informationssicherheitszielen.
d) Rückmeldung von interessierten Parteien
e) Ergebnisse der Risikobeurteilung und Status des Plans für die Risikobehandlung und
f) Möglichkeit zur fortlaufenden Verbesserung.

Die Ergebnisse der Managementbewertung müssen Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung sowie zu jeglichem Änderungsbedarf am Informationssicherheitssystem enthalten.
Die Organisation muss dokumentierte Informationen als Nachweis der Ergebnisse der Managementbewertung aufbewahren.

5.2.4 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.
Die oberste Leitung muss die Verantwortlichkeiten und Befugnisse zuweisen für:
a) Das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieser internationalen Norm erfüllt und
b) Das Berichten an die oberste Leitung über die Leistung des Informationssicherheitsmanagementsystems.

Anmerkung: Die oberste Leitung darf auch Verantwortlichkeiten und Befugnisse für das Berichten der Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zuweisen.

5.2.5 Überwachung, Messung, Analyse & Bewertung

Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten.
Die Organisation muss bestimmen:
a) was überwacht und gemessen werden muss, einschließlich der Informationssicherheitsprozesse und Maßnahmen;
b) die Methode zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

Anmerkung: die ausgewählten Methoden sollten zu vergleichbaren und reproduzierbaren Ergebnissen führen, damit sie als gültig zu betrachten sind.
c) wann die Überwachung und Messung durchzuführen ist;
d) wer überwachen und messen muss;
e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind und
f) wer diese Ergebnisse analysieren und bewerten muss.

Die Organisation muss geeignete dokumentierte Informationen als Nachweis der Ergebnisse aufbewahren.

5.2.6 Dokumentierte Information

Allgemeines

Das Informationssicherheitsmanagementsystem der Organisation muss beinhalten:

a) Die von dieser internationalen Norm geforderte dokumentierte Information und
b) Dokumentierte Information, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems bestimmt hat.

Anmerkung: Der Umfang dokumentierter Information für ein Informationssicherheitsmanagementsystem kann sich von Organisation zu Organisation unterscheiden und zwar aufgrund

1) Der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;
2) Der Komplexität der Prozesse und deren Wechselwirkungen und
3) Der Kompetenz der Personen.

Erstellen und Aktualisieren

Beim Erstellen und Aktualisieren dokumentierter Information muss die Organisation:

a) Angemessene Kennzeichnung und Beschreibung (z.B. Titel, Datum, Autor oder Referenznummer);
b) Angemessenes Format (z.B. Sprache, Softwareversion, Grafiken) und Medium (z.B. Papier, elektronisches Medium) und
c) Angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit

sicherstellen.

Lenkung dokumentierter Information

Die für das Informationssicherheitsmanagementsystem erforderliche und von dieser Internationalen Norm geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie

a) Verfügbar und für die Verwendung geeignet ist, wo und wann sie benötigt wird und
b) Angemessen geschützt wird (z.B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität).

Zur Lenkung dokumentierter Informationen muss die Organisation, falls zutreffend, folgende Tätigkeiten berücksichtigen:

c) Verteilung, Zugriff, Auffindung und Verwendung
d) Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;
e) Überwachung von Änderungen (z.B. Versionskontrolle) und
f) Aufbewahrung und Verfügung über den weiteren Verbleib.

Dokumentierte Information externer Herkunft, die von der Organisation als notwendig für die Planung und den Betrieb des Informationssicherheitsmanagementsystems bestimmt wurde, muss angemessen gekennzeichnet und gelenkt werden.

Anmerkung: Zugriff kann eine Entscheidung voraussetzen, mit der die Erlaubnis erteilt wird, dokumentierte Information lediglich zu lesen, oder die Erlaubnis und Befugnis zum Lesen und Ändern dokumentierter Information usw.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.

6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Maßnahme: Alle Zuständigkeiten der Informationssicherheit sollten festgelegt und zugeordnet sein.

a) Die konkrete Zuweisung der Verantwortlichkeiten einzelner Komponenten/Aspekte ist für jedes System gemäß der Tabelle (Anhang 1) zu dokumentieren.
b) Die Verantwortlichkeiten müssen den Schutz von Werten vor unberechtigtem Zugriff, Offenlegung, Veränderung, Zerstörung oder Beeinträchtigung beinhalten.

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.).

6.1.2 Aufgabentrennung

Maßnahme: Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sollten getrennt werden, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.

Die Aufteilung von Rollen und Verantwortlichkeiten muss in Form eines dokumentierten Konzepts vorliegen.

BSIG-4: Bei der Rollentrennung muss berücksichtigt werden, dass operative und kontrollierende Funktionen nicht von derselben Person ausgeübt werden können, z.B.

- Beantragung, Genehmigung und Umsetzung von Berechtigungen oder IT-Changes
- Entwicklung, Test und Betrieb eines IT-Systems

Im Falle von Rollenkonflikten müssen angemessene kompensierende Kontrollen eingerichtet werden.

6.1.3 Kontakt mit Behörden

Maßnahme: Angemessene Kontakte mit relevanten Behörden sollten gepflegt werden.

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.

6.1.4 Kontakt mit speziellen Interessensgruppen

Maßnahme: Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheits-orientierten Expertenforen und Fachverbänden sollten gepflegt werden.

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.

6.1.5 Informationssicherheit im Projektmanagement

Maßnahme: Informationssicherheit sollte im Projektmanagement berücksichtigt werden, ungeachtet der Art des Projekts.

6.2 Mobilgeräte und Telearbeit

Ziel: Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.

[Mobilgeräte umfassen mobile Geräte jeder Art [Smartphones, Tablets, Laptops, Netbooks usw.]].

6.2.1 Richtlinie zu Mobilgeräten

Maßnahme: Eine Richtlinie und unterstützende Sicherheitsmaßnahmen sollten umgesetzt werden, um die Risiken, welche durch die Nutzung von Mobilgeräten bedingt sind, zu handhaben.

Für den Einsatz von mobilen Geräten sind Regelungen und Verfahren zu erstellen, die mindestens folgende Aspekte berücksichtigen:

a] Physischer Schutz
b] Zugangskontrollen
c] Kryptographische Maßnahmen
d] Backup
e] Virenschutz

Mobile Geräte sind vor unbefugter Nutzung bzw. die darauf gespeicherten Daten vor unberechtigter Einsichtnahme und unautorisiertes ab- bzw. mithören zu schützen. Hierzu zählen insbesondere folgende Maßnahmen:

a] Authentifizierungsmechanismen
b] Verschlüsselung der gespeicherten Informationen
c] Sperrung des Geräts nach einer definierten Zeit
d] Löschung der Daten nach einer definierten Anzahl fehlerhafter Anmeldeversuche
e] **CV:** Die Nutzung unsicherer [= unverschlüsselt] WLAN-Kommunikation muss technisch unterbunden werden.

6.2.2 Telearbeit

Maßnahme: Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sollten umgesetzt sein.

Es sind Regelungen und Verfahren für die Arbeit außerhalb des FMG-Konzern-Standortes mit Remote Access zu einem FMG-Netzwerk umzusetzen. Diese müssen folgende Aspekte berücksichtigen:

a] Berechtigte Geräte [Geräte des FMG-Konzerns, private Geräte etc.]

b) Authentifizierungsverfahren
c) Voraussetzungen für Verbindung mit dem FMG-Netzwerk
d) Management von remote betriebenen Geräten
e) Schutz der Ausstattung und Informationen durch firmenfremde Personen
f) Rückgabe von Ausstattung bzw. Rücknahme von Zugangs-/Zugriffsberechtigungen bei Beendigung der Telearbeit.

7 Personalsicherheit

7.1 Vor der Beschäftigung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.

7.1.1 Sicherheitsüberprüfung

Maßnahme: Alle Personen, die sich um eine Beschäftigung bewerben, sollten einer Sicherheitsüberprüfung unterzogen werden, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.

Bei der Überprüfung sind in Abhängigkeit der vorgesehenen Tätigkeit die nachfolgenden Aspekte zu berücksichtigen:
a) Überprüfung des Lebenslaufs des Mitarbeiters (auf Vollständigkeit und Richtigkeit);
b) unabhängige Identitätsprüfung (Reisepass oder ähnliches Dokument);
c) weiterführende Prüfungen (z. B. Überprüfung der Kreditwürdigkeit, Prüfung auf Vorstrafen im Rahmen eines polizeilichen Führungszeugnisses, Durchführung einer Luftsicherheitsüberprüfung).

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 berücksichtigen.

DVO 2019/1583: Eine normale bzw. erweiterte Zuverlässigkeitsüberprüfung muss für folgenden Personenkreis durchgeführt werden:
- Personen, deren Aufgabengebiet Kontrollen (Zugangskontrollen, Sicherheitskontrollen oder sonstigen Kontrollen)
- Personen, die Personen, die unbegleiteten Zugang zu Luftfracht und Luftpost, Post und Material von Luftfahrtunternehmen, Bordvorräten und Flughafenlieferungen haben, die den erforderlichen Sicherheitskontrollen unterzogen wurden
- Personen, die Administrator-Rechte oder unbeaufsichtigten und unbeschränkten Zugang zu für Zivilluftfahrtzwecke genutzten kritischen informations- und kommunikationstechnischen Systemen und Daten haben.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Maßnahme: In den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern sollten deren Verantwortlichkeiten und diejenigen der Organisation festgelegt werden.

Die Vereinbarungen mit Mitarbeitern und externen Dienstleistern müssen mindestens die nachfolgenden Inhalte berücksichtigen:

a) Unterzeichnung einer Vertraulichkeitsvereinbarung, bevor Zugang zu informationsverarbeitenden Einrichtungen gewährt wird;
b) Verantwortlichkeiten für die Handhabung von Informationen, die von anderen Firmen oder Externen bereitgestellt wurden;
c) Bericht von Sicherheitsvorfällen oder potenziellen Sicherheitsvorfällen sowie anderen Sicherheitsrisiken für die Organisation.

Es ist sicherzustellen, dass Angestellte und externe Dienstleister die relevanten Vertragsklauseln für Informationssicherheit akzeptieren.

7.2 Während der Anstellung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten bezüglich der Informationssicherheit bewusst sind und diesen nachkommen.

7.2.1 Verantwortlichkeiten der Leitung

Maßnahme: Die Leitung sollte von allen Beschäftigten und Auftragnehmern verlangen, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.

Das Management hat sicherzustellen, dass Mitarbeiter sowie externe Dienstleister im Rahmen ihrer Beschäftigung

a) zur Wahrnehmung ihrer Informationssicherheitsaufgaben und –verantwortlichkeiten richtig instruiert sind, bevor ihnen Zugang zu sensitiven Informationen oder Informationssystemen gegeben wird;
b) die erforderlichen Fähigkeiten und Qualifikationen haben und beibehalten.

7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Maßnahme: Alle Beschäftigten der Organisation und, wenn relevant, Auftragnehmer, sollten ein angemessenes Bewusstsein bekommen durch Ausbildung und Schulung sowie
regelmäßige Aktualisierungen zu den Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind.

Anforderung an die Personalentwicklung:

a) Mitarbeiter und externe Dienstleister sind in regelmäßigen Abständen auf relevante Bereiche der Sicherheitsrichtlinien des Unternehmens zu schulen.
b) Mitarbeiter und externe Dienstleister müssen die nötige Fachkunde zur Ausführung
ihrer Tätigkeiten besitzen und sich regelmäßig gemäß aktuellen technischen Standards fortbilden.
c) BSIG-68/CV: Für Personen in sensiblen Tätigkeitsbereichen (z.B. IT-Administratoren, OT-Administratoren, Softwareentwickler, Führungskräfte, Mitarbeiter die finanzielle Transaktionen tätigen dürfen) müssen zielgruppenspezifische Awareness- und Trainingsmaßnahmen etabliert und regelmäßig wiederholt werden in denen die für die Tätigkeit relevantes Wissen (z. B: über Gefährdungen bzw. Bedrohungen, Best Practices in der sicheren Administration bzw. Entwicklung, Auswirklungen und Risiken „unsicherer" Praktiken, ...) adressiert werden.
d) CV: Es müssen regelmäßig (mindestens quartalsweise) Phishing-Simulationen durchgeführt werden um die Awareness der Mitarbeiter zu überprüfen.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Herausbildung des Bewusstseins der Angestellten, ihre Ausbildung und Schulung sollten insbesondere in Übereinstimmung mit den maßgeblichen Sicherheitsfestlegungen der Abkommensanhänge und anderer Dokumente der Internationalen Zivilluftfahrtorganisation (ICAO) erfolgen.
Die Organisation sollte sicherstellen, dass Anwendungsentwickler über Fähigkeiten verfügen, die es ihnen ermöglichen, sichere Anwendungen umzusetzen.

DVO 2019/1583: Personen, die verantwortlich für die Erkennung und Abwehr von Cyberbedrohungen sind, müssen über die erforderlichen Fähigkeiten und Eignung zur wirksamen Wahrnehmung der ihnen zugewiesenen Aufgabe verfügen. Sie werden über relevante Cyberrisiken nach dem Grundsatz 'Kenntnis nur wenn nötig' informiert.

Personen, die Zugang zu Daten oder Systemen haben, müssen geeignete und spezifische aufgabenbezogene Schulungen absolvieren, die ihren Funktionen und Verantwortlichkeiten entsprechen, wobei sie auch über relevante Risiken informiert werden, wenn dies aufgrund ihrer beruflichen Funktion erforderlich ist. Die zuständige Behörde muss den Inhalt der Schulung genehmigen.

7.2.3 Maßregelungsprozess

Maßnahme: Ein formal festgelegter und bekanntgegebener Maßregelungsprozess sollte eingerichtet sein, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.

7.3 Beendigung und Änderung der Beschäftigung

Ziel: Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.

7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Maßnahme: Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, dem Beschäftigten oder Auftragnehmer mitgeteilt und durchgesetzt werden.

Die Verantwortlichkeiten sind im Rahmen eines dokumentierten Prozesses für Austritte zu beschreiben, in dem alle relevanten Schritte enthalten sind.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

8.1.1 Inventarisierung der Werte

Maßnahme: Information und andere Werte, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten erfasst und ein Inventar dieser Werte sollte erstellt und gepflegt werden.

Es muss ein Verzeichnis für mindestens nachfolgende Werte erstellt werden:

a) IT-Systeme (Server, Endgeräte, ...)
b) installierte Software pro System
c) Informationen mit zugehöriger Vertraulichkeitseinstufung

Die Aushändigung relevanter Werte an Angestellte oder externe Dienstleister muss dokumentiert werden. Durch angemessene Vorkehrungen und Maßnahmen wird sichergestellt, dass dieses Inventar vollständig, richtig, aktuell und konsistent bleibt. Änderungen im Inventar werden nachvollziehbar historisiert. Soweit hierzu keine wirksamen Automatismen eingerichtet sind, wird dies durch jährlich stattfindende manuelle Überprüfungen der Inventardaten des Werte sichergestellt.

CV: Es sollten regelmäßige (= monatliche) Discovery-Scans durchgeführt werden um neue unbekannte oder unautorisierte Geräte (Endgeräte, IoT-Geräte, ...) im Firmennetzwerk zu erkennen. Außerdem sollte ein Abgleich der durchgeführten Discovery-Scans mit dem Asset-Inventar durchgeführt werden und sichergestellt werden, dass (zulässige) Geräte im Asset-Inventar aktualisiert werden und nicht mehr benötigte Geräte aus dem Asset-Inventar entfernt werden.

Die genutzten Cloud-Dienste müssen in geeigneter Form in einer Übersicht geführt werden.

8.1.2 Zuständigkeit für Werte

Maßnahme: Für alle Werte, die im Inventar geführt werden, sollte es Zuständige geben.

BSIG-6: Für jeden inventarisierten Wert muss ein Eigentümer definiert und dokumentier werden. **CV:** Dies gilt gleichermaßen für intern entwickelte, als auch für gekaufte IT-Systeme. Der Eigentümer ist über den gesamten Lebenszyklus des Werts (= Beschaffung, Inbetriebnahme, Betrieb & Wartung, rechtzeitiges Ausphasen, z.B: bei EoL-Systemen) zuständig.

Der Eigentümer eines Wertes muss verantwortlich sein, dass
a) Informationen und Systeme entsprechend den Vorgaben klassifiziert werden;
b) eine Definition und regelmäßige Überprüfung der Zugangs-/Zugriffsbeschränkungen und Klassifikation der Werte, unter Berücksichtigung der anwendbaren Zugangskontrollpolitiken, erfolgt.

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.

8.1.3 Zulässiger Gebrauch von Werten

Maßnahme: Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten aufgestellt, dokumentiert und angewendet werden.

8.1.4 Rückgabe von Werten

Maßnahme: Alle Beschäftigten und sonstige Benutzer, die zu externen Parteien gehören, sollten bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehörten, zurückgeben.

8.2 Informationsklassifizierung

Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.

8.2.1 Klassifizierung von Information

Maßnahme: Informationen sollte anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert werden.

Zusätzliche Vorgaben zur Klassifikation und Nutzung von Informationen sind in der IT-Nutzungsrichtlinie festgelegt.

Bei der Klassifizierung von Informationen sind gesetzliche, aufsichtsrechtliche sowie vertragliche Anforderungen zu berücksichtigen.

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.

8.2.2 Kennzeichnung von Information

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

a) Beim Ausdrucken von Informationen muss eine explizite Kennzeichnung möglich sein.
b) Beim Datenexport müssen die exportierten Daten explizit gekennzeichnet werden können.
c) Festplatten von mobilen Geräten wie Notebooks bzw. Datenspeicher von Smartphones oder Tablets, auf denen vertrauliche Informationen gespeichert sind, müssen verschlüsselt werden. Dies gilt auch für Datenträger wie z. B. CDs, DVDs, USB-Sticks oder externe Festplatten.
d) Vertrauliche oder streng vertrauliche Informationen müssen bei Übertragung in oder durch öffentliche Netze verschlüsselt werden. Hierzu müssen Lösungen verwendet werden, die auf dem aktuellen Stand der Technik basieren.

e) Eine Speicherung von vertraulichen bzw. streng vertraulichen Daten (z. B. Datenbank-Kennwörtern) im Klartext im Code bzw. Konfigurationsdateien ist nicht zulässig.
f) Auf mobilen Geräten muss eine Verschlüsselung der lokalen Daten aktiviert sein.
g) Vertrauliche bzw. streng vertrauliche Daten dürfen nicht auf unverschlüsselten Clientrechnern abgelegt werden.

8.2.3 Handhabung von Werten

Maßnahme: Verfahren für die Handhabung von Werten sollten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die relevanten Regelungen eingehalten werden.

8.3 Handhabung von Datenträgern

Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist, wird unterbunden.

8.3.1 Handhabung von Wechseldatenträgern

Maßnahme: Verfahren für die Handhabung von Wechseldatenträgern sollten entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt werden.

Bezüglich des Umgangs mit vertraulichen Informationen auf Datenträgern muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „IT-Nutzungsrichtlinie“ eingehalten werden.

CV: Beim (autorisierten) Einsatz von Wechseldatenträgern muss dessen Verwendung protokolliert bzw. überwacht werden um einen ungewünschten Datenabfluss zu verhindern bzw. zu erkennen.

8.3.2 Entsorgung von Datenträgern

Maßnahme: Nicht mehr benötigte Datenträger müssen sicher und unter Anwendung formaler Verfahren entsorgt werden.

Es müssen Maßnahmen zur sicheren Löschung oder Entsorgung von Datenträgern zur Verfügung gestellt oder alternative organisatorische/vertragliche Maßnahmen zur sicheren Löschung/Entsorgung von Datenträgern ergriffen werden.
Dies beinhaltet die Anwendung von angemessenen Löschverfahren einschließlich der Nachvollziehbarkeit der ordnungsgemäßen Durchführung.
Der Schutz der Informationen muss gewährleistet werden, auch wenn IT-Systeme bzw. darin enthaltene Datenspeicher nicht länger verwendet werden, nicht länger innerhalb des FMG-Konzerns verwendbar sind oder wenn sie zu einem anderen Zweck verwendet werden.

8.3.3 Transport von Datenträgern

Maßnahme: Datenträger, die Information enthalten, müssen während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden.

Sofern Datenspeicher transportiert werden, müssen die darauf gespeicherten Daten mit einem Verfahren entsprechend dem aktuellen Stand der Technik verschlüsselt sein.

Die für die Entschlüsselung erforderlichen Informationen müssen auf einem anderen Kommunikationsweg zum Empfänger übermittelt werden wie der Datenspeicher.
Der Transport von Medien mit Informationen der Klasse „Vertraulich" oder „Streng vertraulich" muss dokumentiert werden. Es muss sichergestellt sein, dass der Aufenthaltsort des Datenspeichers zu jeder Zeit bekannt ist (z. B. Carrier mit Paket-Tracking).

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangssteuerung

Ziel: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt.

9.1.1 Zugangssteuerungsrichtlinie

Maßnahme: Eine Zugangssteuerungsrichtlinie muss auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft werden.

Es ist ein Regelwerk zur Zugangskontrolle für IT-Systeme zu erstellen, welches mindestens die nachfolgenden Anforderungen erfüllt, um sicherzustellen, dass unbefugte Nutzung ausgeschlossen wird.
Jedes IT-System muss über angemessene Authentifizierungsmechanismen verfügen, welches für alle Nutzer gültig ist.
Der Informationsverantwortliche bzw. von diesen autorisierte Mitarbeiter legen in enger Abstimmung mit dem Produktmanager fest, welche Personen Zugangsberechtigung zu einem IT-System erhalten.
Einem Nutzer dürfen nur genau die Zugangs- und Zugriffsrechte eingeräumt werden, die er zum Erfüllen seiner Aufgaben benötigt.
Die Genehmigung, Umsetzung und Verwaltung von Zugangs- und Zugriffsrechten sollte nach dem Prinzip der Trennung von Verantwortlichkeiten („Separation of Duties" oder „Vier-Augen-Prinzip") ausgeführt werden.
Trennung der Rollen und Funktionen für die Erteilung von Zugangsrechten in Bezug auf Genehmigung und Rechteverwaltung.

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Maßnahme: Benutzer müssen ausschließlich Zugang auf diejenigen Netzwerke und Netzwerkdienste haben, zu deren Nutzung sie ausdrücklich befugt sind.

Es ist ein Regelwerk für die Nutzung von Netzen und Netzdiensten zu erstellen, welches mindestens die nachfolgenden Punkte beinhaltet:
a) die Netze und Netzdienste, auf die zugegriffen werden darf,
b) Berechtigungsverfahren, um festzustellen, wer auf welche Netze und Netzdienste zugreifen darf,
c) Administrations-Maßnahmen und Prozeduren, um den Zugang zu Netzen und Netzdiensten zu schützen.

9.2 Benutzerzugangsverwaltung

Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.

9.2.1 Registrierung und Deregistrierung von Benutzern

Maßnahme: Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern muss umgesetzt werden, um die Zuordnung von Zugangsrechten zu ermöglichen.

Um eine Nachvollziehbarkeit zu gewährleisten, müssen Zugangs- und Zugriffsrechte sowie deren Erteilung und Entzug in geeigneter Weise dokumentiert sein.
Bei Beendigung des Arbeitsverhältnisses muss ein sofortiger Entzug der vorhandenen Zugangs- und Zugriffsrechte gemäß den Vorgaben des Personalbereichs sichergestellt werden.
Bei der Vergabe von Zugangsberechtigungen ist darauf zu achten, dass ausschließlich eindeutige Benutzerkennungen vergeben werden, um sicherzustellen, dass Benutzer einer Benutzerkennung zuordenbar sind. Die Verwendung von Gruppenkennungen ist nur dann zulässig, wenn dies aus betrieblichen oder geschäftlichen Gründen notwendig ist und dies genehmigt sowie dokumentiert wurde.
Anonyme Administrations-Accounts (z. B. Windows: Administrator oder Unix: Root) müssen grundsätzlich durch persönliche Administrations-Accounts ersetzt werden, die eindeutig einer bestimmten Person zugeordnet werden können. Sofern dies für sicherheitskritische IT-Systeme nicht möglich ist, muss die Nutzung von anonymen Administrations-Accounts protokolliert werden.
Darüber hinaus ist sicherzustellen, dass die Passwörter für anonyme Administrations-Accounts mindestens einmal jährlich sowie unverzüglich bei Ausscheiden eines Nutzers dieser Accounts geändert werden. Für sicherheitskritische Systeme sind die Zugangsdaten dieser Accounts in einem versiegelten Umschlag in einem abschließbaren Schrank (oder einem Safe) aufzubewahren. Der Zugriff auf diese Informationen muss geregelt und dokumentiert werden.

9.2.2 Zuteilung von Benutzerzugängen

Maßnahme: Ein formaler Prozess zur Zuteilung von Benutzerzugängen muss umgesetzt werden, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.

Es müssen Benutzerkonten mit den geringsten möglichen Privilegien und Zugriffsrechten auf Systemebene verwendet werden. Dazu gehören beispielsweise Zugriffsrechte auf Dateien, Ordner, Geräte im Netz, Datenbankobjekte oder Ereignisprotokolle.
Es ist ein Verfahren für die Reaktivierung gesperrter Accounts sowie die Rücksetzung von Passwörtern zu etablieren.
Bei internen Versetzungen bzw. Neuzuordnungen von Aufgaben muss eine zeitnahe Änderung von Zugangs- und Zugriffsrechten sichergestellt werden.
Zugangsrechte sind in Abhängigkeit des Nutzerstatus unbefristet (interne Mitarbeiter) oder befristet (z. B. externe Mitarbeiter, Geschäftspartner, Auszubildende, Werkstudenten, Praktikanten) zu erteilen.
BSIG-27: Sammelaccounts für Benutzer dürfen aus Gründen der Nachvollziehbarkeit nicht verwendet werden.

9.2.3 Verwaltung privilegierter Zugangsrechte

Maßnahme: Zuteilung und Gebrauch von privilegierten Zugangsrechten muss eingeschränkt und gesteuert werden.

Es muss sichergestellt werden, dass privilegierte Zugangsrechte nur bei tatsächlichem Bedarf vergeben werden.
Die mit jeder Systemkomponente (z. B. Betriebssysteme, Datenbanken und Anwendungen) verbundenen Sonderrechte und die Benutzer, denen diese Sonderrechte zugeteilt werden, müssen dokumentiert sein.
Sonderrechte dürfen nur einer von der normalen Benutzerkennung für den Alltagsgebrauch getrennten Benutzerkennung zugewiesen werden.

Für Cloud-Dienste müssen soweit möglich Notfallkonten eingerichtet und mit folgenden Maßnahmen geschützt werden:
- Es muss sich um Cloud-only Konten handeln (für den Fall, dass das zentrale Identitätsmanagement der FMG ausfällt)
- Es sind mindestens jährliche Passwortwechsel zu planen

- Die MFA Nutzung muss abgewogen werden, da im Notfall MFA nicht funktionieren könnte
- Die Nutzung eines Notfallkontos muss zu einem Monitoring-Alarm führen (IT-Betrieb und CDC)
- Nach Nutzung des Notfallkontos muss das Passwort gewechselt werden

9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

Maßnahme: Die Zuordnung von geheimer Authentisierungsinformation muss über einen formalen Verwaltungsprozess gesteuert werden.

Passwörter von privilegierten Kennungen (z. B. Administratoren) müssen für Notfälle einem definierten Vertreterkreis zugänglich sein und an einem besonders geschützten Ort aufbewahrt werden.
Standardpasswörter der Hersteller müssen nach der Installation von Systemen oder Software geändert werden.
Ein Passwort- bzw. PIN-Schutz muss auch auf mobilen Geräten vorhanden sein, sobald ein Zugriff auf Informationen des FMG-Konzerns erfolgt.
Benutzer müssen grundsätzlich mit einem individuellen Initialpasswort versorgt werden, welches bei der Erstanmeldung geändert werden muss. **BSIG-26:** Wird ein Initialpasswort nicht innerhalb von 14 Tage geändert, muss der Zugang gesperrt werden.
Passwörter dürfen ausschließlich dem jeweiligen Accountinhaber auf sichere Art und Weise mitgeteilt werden.
Passwörter dürfen nur durch geeignete Maßnahmen (z. B. Hashing) geschützt gespeichert werden.
Die Rücksetzung von Passwörtern darf nur unter Einhaltung eines genehmigten Verfahrens zur Identitätsprüfung erfolgen.
Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) erfolgt in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt.

9.2.5 Überprüfung von Benutzerzugangsrechten

Maßnahme: Die für Werte Zuständigen sollten in regelmäßigen Abständen die Benutzerzugangsrechte überprüfen.

Der Informationsverantwortliche muss regelmäßig die erteilten Berechtigungen überprüfen und festgestellten Änderungsbedarf umgehend umsetzen bzw. initiieren.
a) Benutzer-Accounts (normale Berechtigung) müssen mindestens jährlich gereviewt werden
b) privilegierte Accounts mindestens halbjährlich gereviewt werden.
Die durchgeführte Prüfung ist in geeigneter Weise zu dokumentieren.

9.2.6 Entzug oder Anpassung von Zugangsrechten

Maßnahme: Die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen sollten bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst werden.

BSIG-61/CV: Eine sofortige Anpassung von Berechtigungen (betrifft sowohl Benutzerkonten als auch die verschiedenen Berechtigungen, die für ein Benutzerkonto vergeben wurden) bei personellen Änderungen muss sichergestellt werden.

Dabei muss für externe Benutzerkonten bereits bei der Anlage / Vergabe der Berechtigung ein Auslaufdatum (Datum an dem ein Benutzerkonto deaktiviert wird, sofern dies nicht manuell verlängert wird) festgelegt wer-

den. Ist das geplante Auftragsende bereits bei Anlage / Vergabe der Berechtigung bekannt, muss das Auslaufdatum für das Benutzerkonto mit Ende der Beauftragung zu setzen. Dieses Auslaufdatum für externe Benutzerkonten darf einen Zeitraum von 6 Monaten nicht überschreiten.

Dabei muss bedarfsweise unterschieden werden, wie, aus welchem Grund bzw. durch wen die Beendigung oder Änderung eingeleitet wurde.

9.2.7 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 zur Umsetzung (gem. CoPiP 3.2):

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.

Werden Identitäten mit Cloud-Diensten synchronisiert, dürfen keine administrativen Identitäten (Admin-Accounts (T0, T1, T2)) synchronisiert werden.

Es sollte bewertet werden, ob die Anbindung an ein zentrales IAM der FMG durchgeführt werden soll. Die Bewertung muss dokumentiert werden.

9.2.8 Organisationsübergreifende eindeutige Darstellung von Entitäten

Maßnahme: Im organisationsübergreifenden Identitätsmanagement sollten die Entitäten einheitlich dargestellt werden.

Anleitung zur Umsetzung (gem. CoPiP 3.2):

Im organisationsübergreifenden Identitätsmanagement sollten folgende Entitäten betrachtet werden:

- Menschen
- Organisationseinheiten und organisatorische Rollen (Departments)
- 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.

9.3 Benutzerverantwortlichkeiten

Ziel: Benutzer sind für den Schutz Ihrer Authentisierungsinformation verantwortlich gemacht.

9.3.1 Gebrauch geheimer Authentisierungsinformation

Maßnahme: Benutzer sollten verpflichtet werden, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.

Benutzer müssen ihre Passwörter umgehend ändern, wenn deren Vertraulichkeit in irgendeiner Form gefährdet wurde.
Für IT-Systeme, bei denen eine vermutete oder festgestellte Kompromittierung vorliegt, ist sicherzustellen, dass die Passwörter sämtlicher betroffenen bzw. potenziell betroffenen Benutzerkonten umgehend geändert werden.
Passwörter für Administrations-Accounts dürfen nicht für andere Zwecke verwendet werden.
Es ist sicherzustellen, dass Passwörter nicht im Klartext in Dokumentationen enthalten sind.
Als Schutzmaßnahme gegen Social Engineering Angriffe dürfen Administratoren generell nie die Passwörter von Nutzern erfragen, sondern müssen diese im Supportfall technisch zurücksetzen.

9.4 Zugangssteuerung für Systeme und Anwendungen

Ziel: Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.

9.4.1 Informationszugangsbeschränkung

Maßnahme: Zugang zu Information und Anwendungssystemfunktionen sollte entsprechend der Zugangssteuerungsrichtlinie eingeschränkt sein.

Zugriffsberechtigungen auf Dateien müssen in allen IT-Systemen standardmäßig so gesetzt werden, dass nicht autorisierten Personen der Zugriff verwehrt wird.
Die Zugriffsrechte von Benutzern oder anderen Anwendungen sind gemäß den geschäftlichen Anforderungen einzuschränken und zu kontrollieren.

9.4.2 Sichere Anmeldeverfahren

Maßnahme: Soweit es die Zugangssteuerungsrichtlinie erfordert, sollte der Zugang auf Systeme und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert werden.

- Um zu vermeiden, dass Passwörter erraten werden, ist nur eine maximale Anzahl von 10 fehlerhaften Versuchen bei der Eingabe von Passwörtern zuzulassen.
- Wird diese Grenze überschritten, muss der Account gesperrt werden und darf anschließend nur gemäß dem festgelegten Prozess zum Entsperren von Accounts wieder freigeschaltet werden.
- Wenn ein Teil der Anmeldung an einem IT-System fehlschlägt, darf der Benutzer lediglich darüber informiert werden, dass der Anmeldevorgang insgesamt fehlgeschlagen ist. Er darf nicht darüber informiert werden, welcher Teil der Anmeldung (Benutzername oder Passwort) fehlgeschlagen ist.
- Das eingegebene Passwort darf standardmäßig nicht vollständig bei der Eingabe angezeigt werden.

- Soweit technisch möglich sollte der Einsatz von Multifaktor-Authentisierung (MFA) gegenüber der Verwendung von Benutzername und Kennwort zur Authentisierung bevorzugt werden.
- Bei der Nutzung von Cloud-Diensten muss der Einsatz von Multifaktor-Authentisierung (MFA) für alle Accounts/Zugriffe, welche außerhalb des FMG Netzwerkes genutzt werden können, technisch erzwungen werden.

BSIG-27: Es dürfen lediglich sichere, d.h. anerkannte Anmeldeverfahren gem. Stand-der-Technik eingesetzt werden.

BSIG-27/CV: Eine Multifaktor-Authentisierung (MFA) muss für alle Accounts mit privilegierten Zugangsberechtigungen technisch erzwungen werden, sofern ein Zugriff über öffentliche Netze erfolgt. Für T0-Accounts muss eine MFA immer erzwungen werden. Dies gilt gleichermaßen für IT-Systeme, als auch für OT-/Scada-/ICS-Systeme. Sofern kein technisches Erzwingen erfolgt (oder erfolgen kann) müssen angemessene kompensierende Maßnahmen umgesetzt werden.

9.4.3 System zur Verwaltung von Kennwörtern

Maßnahme: Systeme zur Verwaltung von Kennwörtern sollten interaktiv sein und starke Kennwörter sicherstellen.

Die nachstehenden Anforderungen müssen bei allen Systemen beachtet werden, bei denen die Authentisierung ausschließlich über Benutzername und Kennwort erfolgt (ohne zusätzliches Medium, wie z.B. Ausweis):

Regelung für alle Systeme außer mobile Endgeräte:
Soweit technisch möglich, muss erzwungen werden, dass nur sichere Passwörter gewählt werden. Für sichere Passwörter auf allen Systemen (ausgeschlossen mobile Endgeräte) müssen grundsätzlich folgende Anforderungen beachtet werden:

- Mindestlänge 12 Zeichen
- Komplexität: 3 aus 4
- History: 12
- Änderungsintervall: 180 Tage
- Account Lockout: Auto lockout für 30 Min
- keine Trivial-Ersetzung (a=@, i=1)
- keine Verwendung von Worten aus Wörterbüchern (Sommer2019)
- Passwörter werden bei Änderungen nicht hochgezählt (Sommer2020)
- Mindestalter 1 Tag

Regelung für mobile Endgeräte:
Soweit technisch möglich, muss erzwungen werden, dass nur sichere Passwörter gewählt werden. Für sichere Passwörter auf mobilen Endgeräte müssen grundsätzlich folgende Anforderungen beachtet werden:

- Mindestlänge 6 Zeichen
- History: 10
- Änderungsintervall: 180 Tage
- Account Lockout: Auto lockout für 30 Min
- Mindestalter 1 Tag
- Maximale Anzahl an Fehlversuche: 6

Für besondere Berechtigungen (Funktionskonten, privilegierte und hoch privilegierte Konten) müssen soweit technisch möglich höhere Sicherheitsanforderungen (z. B. längere Passwörter, kürzeres Änderungsintervall, höhere Komplexität, MFA) erzwungen werden.

9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Maßnahme: Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, sollte eingeschränkt und streng überwacht werden.

BSIG-30: Die Verwendung von Dienstprogrammen und Managementkonsolen, die weitreichenden Zugriff auf Informationen haben, muss auf ein Mindestmaß beschränkt werden (nur autorisierter Personenkreis). Vergabe und Änderung entsprechender Zugriffsberechtigungen erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Der Zugriff auf solche Hilfsprogramme muss mittels MFA abgesichert sein.

9.4.5 Zugangssteuerung für Quellcode von Programmen

Maßnahme: Zugang zu Quellcode von Programmen sollte eingeschränkt werden.

BSIG-31: Der Zugriff zu Quellcode und ergänzende für die Entwicklung relevante Informationen muss restriktiv sein und überwacht werden, um die Einführung von nicht-autorisierten Funktionen oder Änderungen zu vermeiden.

9.4.6 Web-Application Firewalls

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

Anleitung zur Umsetzung (gem. CoPiP 3.2):

- 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 Regeln), 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 Regeln) 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 Regeln auf HTTP/HTTPS-Nachrichtenübermittlungen anzuwenden, um viele Angriffsversuche erkennen und blockieren zu können.

10 Kryptographie

10.1 Kryptographische Maßnahmen

Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt.

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Maßnahme: Eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information sollte entwickelt und umgesetzt werden.

Es muss eine Kryptorichtlinie erstellt werden, die mindestens die nachfolgenden Punkte berücksichtigt:

a) Anwendung von Verschlüsselung zum Schutz sensitiver Informationen, die auf Endgeräten, mobilen Datenträgern oder über Kommunikationsverbindungen transportiert werden,
b) Auswirkungen, die eine Verwendung verschlüsselter Informationen auf Maßnahmen hat, die von der Untersuchung des Inhalts von Informationen abhängig sind (z. B. Virenscanner),
c) Ansatz zur Schlüsselverwaltung, inklusive Methoden, um kryptographische Schlüssel zu schützen und verschlüsselte Informationen zurückzugewinnen, falls der Schlüssel verloren, kompromittiert oder beschädigt wurde.
d) Für die Nutzung von Kryptografie müssen die bewährten Kryptographieservices oder Bibliotheken, die im Betriebssystem oder in der Laufzeitumgebung enthalten sind, verwendet werden. Es dürfen keine eigenen Verfahren entwickelt werden.
e) Daten müssen so lange wie möglich verschlüsselt belassen werden.
f) Klartextdaten sind in so wenig Variablen wie möglich abzuspeichern.

Passende Algorithmen und erforderliche Schlüssellängen müssen entsprechend den Sicherheitsanforderungen gewählt werden. Sicherheit steigt mit der Schlüssellänge. Empfohlen ist eine AES-basierte Verschlüsselung.

Für alle in Cloud-Diensten verwendeten Web- sowie Multicast-Protokolle müssen ausschließlich anerkannte Verschlüsselungsverfahren gemäß Kapitel Schlüsselverwaltung eingesetzt werden.

Die Datenverschlüsselung der Daten beim Cloud-Anbieter (Data at Rest) muss aktiviert werden und es dürfen ausschließlich anerkannte Verschlüsselungsverfahren gemäß Kapitel Schlüsselverwaltung eingesetzt werden. Hierbei sind je nach Verwendungszweck die Systeme zur Schlüsselverwaltung des Cloud-Anbieters zu nutzen oder die Schlüsselverwaltung der FMG.

10.1.2 Schlüsselverwaltung

Maßnahme: Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln sollte entwickelt und über deren gesamten Lebenszyklus umgesetzt werden.

Für Kryptografie dürfen ausschließlich anerkannte Verschlüsselungsverfahren eingesetzt werden (z. B. AES, RSA)
Bei den kryptografischen Verfahren sind folgende Mindestschlüssellängen zu gewährleisten:

a) bei symmetrischen Verfahren mindestens 256 bit
b) bei asymmetrischen Verfahren mindestens 2048 bit

Eine Veröffentlichung von geheimen Schlüsseln an Dritte ist nicht gestattet. Ebenso dürfen Passwörter, die ggf. den Zugang zu Schlüsselmaterial gewähren, nicht weitergegeben werden.
Die Verteilung von kryptografischen Schlüsseln muss auf einem sicheren Weg erfolgen.
Öffentliche Schlüssel sind in einem zentralen Verzeichnis direkt oder indirekt zugänglich für alle Nutzer des Dienstes abzulegen.
Private Schlüssel sind ausschließlich dem entsprechenden Benutzer zugänglich zu machen. Dies kann auch mittelbar über eine Software erfolgen.
Von allen Schlüsseln sind seitens IT Sicherungskopien vorzuhalten. Administratoren mit Zugriff auf diese Sicherungskopien dürfen keinen Zugriff auf verschlüsselte Daten erhalten (Funktionstrennung).

Bei Erzeugung von Schlüsseln soll – soweit technisch und rechtlich möglich – die Verwendung eines Generalschlüssels implementiert werden. Der Generalschlüssel kann dann alle verschlüsselten Daten aller Anwender des Dienstes entschlüsseln.
Die Nutzung eines Generalschlüssels darf nicht einer einzelnen Person möglich sein.
Der Zugriff auf private Schlüssel von Nutzern sowie auf Generalschlüssel durch Administratoren ist grundsätzlich nicht erlaubt.
In begründeten Ausnahmefällen kann IT auf private Schlüssel eines Nutzers oder auf den Generalschlüssel zugreifen und Daten eines Nutzers entschlüsseln, ohne den Nutzer vorab zu informieren. Ein begründeter Ausnahmefall liegt insbesondere vor bei:

a) Unvorhergesehenem Ausscheiden aus dem Unternehmen (z. B. fristlose Kündigung, Tod)
b) Voraussichtlich längerer Abwesenheit vom Arbeitsplatz ohne Möglichkeit des Kontakts mit dem Betroffenen (z. B. Erkrankung, Unfall), bei unaufschiebbarer Erforderlichkeit des Zugriffs auf verschlüsselte Daten
c) Soweit in einem behördlichen oder gerichtlichen Verfahren zur Wahrung der Interessen des FMG-Konzerns erforderlich.

Dieser unangekündigte Zugriff auf verschlüsselte Daten eines Nutzers unterliegt einem besonderen Verfahren, in dem die Verhältnismäßigkeit der Maßnahme durch Einbeziehung des Datenschutzbeauftragten und eines Mitglieds der jeweils zuständigen Arbeitnehmervertretung überprüft wird.
Betroffene Nutzer sind über den Zugriff auf die verschlüsselten Daten in den beschriebenen Fällen unverzüglich in Kenntnis zu setzen, sobald Natur und Zweck der Maßnahme dies gestatten.

11 Physische und umgebungsbezogene Sicherheit

11.1 Sicherheitsbereiche

Ziel: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.

11.1.1 Physische Sicherheitsperimeter

Maßnahme: Zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitsperimeter festgelegt und verwendet werden.

11.1.2 Physische Zutrittssteuerung

Maßnahme: Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung geschützt werden, um sicherzustellen, dass nur berechtigtes Personal Zutritt hat.

a) Personen ohne eigene Zutrittsberechtigung zur jeweiligen Zone müssen grundsätzlich während ihres Aufenthaltes von einem autorisierten Mitarbeiter begleitet werden.
b) Mitarbeiter externer Firmen müssen durch den Vertragspartner vorab benannt werden. Alternativ muss er eine Identifikation als Mitarbeiter oder Dienstleister der externen Firma vorlegen können.

11.1.3 Sichern von Büros, Räumen und Einrichtungen

Maßnahme: Die physische Sicherheit für Büros, Räume und Einrichtungen muss konzipiert und angewendet werden.

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Maßnahme: Physischer Schutz vor Naturkatastrophen, bösartigen Angriffen oder Unfällen sollte konzipiert und angewendet werden.

Materialien mit hoher Brandlast (z. B. leicht entzündliche Stoffe, Papier) dürfen nicht in Info- oder Serverräumen sowie Rechenzentren gelagert werden.
Geeignete Ausstattung zur Brandbekämpfung ist bereitzustellen und adäquat zu platzieren.

BSIG-74: Räume, bzw. Gebäude in denen sich kritische Informationen, IT-Systeme oder IT-Infrastruktur befinden müssen vor relevanten Umweltbedrohungen (z.B. Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen, ...) angemessen geschützt werden. Dazu müssen angemessene Maßnahmen (Raumüberwachung, Brand-Früherkennung bzw. Brand-Frühesterkennung, ...) umgesetzt werden.

11.1.5 Arbeiten in Sicherheitsbereichen

Maßnahme: Verfahren für das Arbeiten in Sicherheitsbereichen sollten konzipiert und angewendet werden.

11.1.6 Anlieferungs- und Ladebereiche

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

11.2 Geräte und Betriebsmittel

Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Maßnahme: Geräte und Betriebsmittel sollten so platziert und geschützt werden, dass Risiken durch umweltbedingte Bedrohungen und Gefahren sowie Möglichkeiten des unbefugten Zugangs verringert sind.

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 Netzwerkdosen usw.

11.2.2 Versorgungseinrichtungen

Maßnahme: Geräte und Betriebsmittel sollten vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.

BSIG-71: Die Versorgung der für den Betrieb erforderlichen IT-Systeme muss gewährleistet sein, überwacht und dessen Funktionsfähigkeit regelmäßig getestet werden (z.B. Elektrizität, Temperatur- und Feuchtigkeitskontrolle, Telekommunikation und Internetverbindung, ...)

11.2.3 Sicherheit der Verkabelung

Maßnahme: Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung sollten vor Unterbrechung, Störung oder Beschädigung geschützt werden.

11.2.4 Instandhaltung von Geräten und Betriebsmitteln

Maßnahme: Geräte und Betriebsmittel sollten ordnungsgemäß instand gehalten werden, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.

Das Erfordernis und der Umfang von Instandhaltungs- und Wartungsmaßnahmen für relevante Gerätschaften muss überprüft und festgelegt werden.

BSIG-71: Sämtliche Wartungsarbeiten müssen in Übereinstimmung mit den von den Lieferanten/Hersteller empfohlenen Wartungsintervallen und -Vorgaben durchgeführt werden. Außerdem dürfen Wartungsarbeiten ausschließlich von autorisiertem Personal durchgeführt werden. Wartungsprotokolle müssen als Nachweise für die ordnungsgemäße Durchführung von Wartungsarbeiten aufbewahrt werden.
BSIG-76: Fernwartung sollte (falls möglich) vermieden werden. Sofern eine Fernwartung durchgeführt wird, muss sichergestellt, dass der Zugriff sicher erfolgt.

11.2.5 Entfernen von Werten

Maßnahme: Geräte, Betriebsmittel, Informationen oder Software sollten nicht ohne vorherige Genehmigung vom Betriebsgelände entfernt werden.

Betriebsmittel, Informationen oder Software dürfen nicht unberechtigt aus dem Standort entfernt werden. Mitarbeiter, Vertragspartner und Externe, die die Mitnahme von Betriebsmitteln genehmigen dürfen, müssen eindeutig festgelegt sein.

11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Maßnahme: Werte außerhalb des Standorts sollten gesichert werden, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.

Systeme und Datenträger, die außerhalb des Standortes mitgenommen werden, dürfen in der Öffentlichkeit nicht unbeaufsichtigt sein.

BSIG-12: Werte (Geräte, Hardware, Software oder Daten) dürfen nur nach ausdrücklicher Genehmigung in externe Räumlichkeiten überführt werden. Die Überführung muss auf sicherem Wege erfolgen (siehe Kap. 8.3.3). Für Werte, die in externen Räumlichkeiten betrieben werden sollte auch der Standort des Werte im Asset-Register dokumentiert werden (siehe Kap. 8.1.1).

11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

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

11.2.8 Unbeaufsichtigte Benutzergeräte

Maßnahme: Benutzer sollten sicherstellen, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt sind.

Es sind geeignete Maßnahmen zum Schutz unbeaufsichtigter IT-Systeme vor unbefugtem Zugriff zu etablieren (z. B. Abmeldung vom System, aktive Sperrung des Gerätes, Aktivierung eines Bildschirmschoners mit automatischer Sperre des betreffenden IT-Systems nach einer definierten Zeitspanne).
Darüber hinaus sind Maßnahmen zum physischen Schutz von IT-Systemen in öffentlich zugänglichen Bereichen zu ergreifen.

11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Maßnahme: Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren für informationsverarbeitende Einrichtungen sollten angewendet werden.

12 Betriebssicherheit

12.1 Betriebsabläufe und –verantwortlichkeiten

Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.

12.1.1 Dokumentierte Betriebsabläufe

Maßnahme: Die Betriebsverfahren sollten dokumentiert und allen Benutzern, die sie benötigen, zugänglich sein.

Der Produktmanager ist verantwortlich für die Erstellung und Pflege einer Betriebsdokumentation für sämtliche IT-Systeme seines Zuständigkeitsbereichs. Diese muss auf einer hohen Abstraktionsebene die Komponenten und Voraussetzungen der jeweiligen IT-Systeme beschreiben, die für einen zuverlässigen Betrieb erforderlich sind.
Die Betriebsdokumentation muss mindestens die nachfolgenden sicherheitsrelevanten Themen enthalten:

a) Betrieb und Wartung
b) Umgang mit Informationssicherheitsereignissen/-vorfällen
c) Änderungsmanagement und Freigabeprozesse
d) Verantwortlichkeiten
e) Logging & Monitoring
f) Externe Partner (Dienstleister, Lieferanten etc.)

12.1.2 Änderungssteuerung

Maßnahme: Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen sollten gesteuert werden.

Eine geregelte Durchführung beinhaltet eine für Dritte nachvollziehbare Dokumentation.
Ein Change Management Prozess muss eingerichtet sein, um sicherzustellen, dass Änderungen an den IT-Systemen durch die verantwortlichen Teams in einer ordnungsgemäßen Art und Weise durchgeführt und mögliche Auswirkungen der Änderungen identifiziert werden.

Bevor Änderungen an IT-Systemen vorgenommen werden, sind diese hinsichtlich Funktionsfähigkeit und Wechselwirkungen mit anderen Systemen zu testen. Soweit möglich, ist dies auf entsprechenden Testsystemen vorzunehmen.
Jede Änderung muss kategorisiert werden und Aufschluss darüber geben, welche Änderungen als wichtige Änderung (major change) eingestuft sind.
Alle wichtigen Änderungen müssen dokumentiert und mindestens sechs Monate lang rückverfolgbar sein. Diese Dokumentation kann in Form der Protokollierung mit Tools, über die Verwendung von Tickets oder in manueller Form erfolgen.

Die Nutzung eines neuen Cloud-Dienstes muss frühzeitig mit dem CDC abgestimmt werden, um eine mögliche Einbeziehung in die Incident Management Prozesse der FMG abzustimmen.

Beim Change Management Prozess müssen die Besonderheiten bei Commercial of the shelf (COTS) Diensten in der Cloud beachtet werden:

- Updates werden durch den Cloud-Anbieter durchgeführt. Die FMG hat hierbei nur die Wahl das Update zu akzeptieren oder den Dienst nicht mehr zu nutzen.
- Da Cloud-Umgebungen typischerweise deutlich häufiger geändert werden, muss dies im Change-Management abgebildet sein. Dies beinhaltet neue Funktionen der Dienste sowie die Abschaltung vorhandener Dienste.
- Der Fokus der Updates der Cloud-Anbieter liegt typischerweise auf der Funktionalität. Updates müssen daher zeitnah auf Implikationen für die IT-Sicherheit überprüft werden.
- Durch Updates kann es zu Änderungen an den bereits vorgenommenen Konfigurationen kommen oder es bestehen neue Konfigurationsmöglichkeiten.

Sofern individuelle Vereinbarungen mit dem Cloud-Anbieter möglich sind, sollten diese auf Basis dieser Richtlinie entworfen werden.

12.1.3 Kapazitätssteuerung

Maßnahme: Die Ressourcennutzung/Benutzung von Ressourcen sollte überwacht und abgestimmt werden, und es sollten Prognosen zu zukünftigen Kapazitätsanforderungen erstellt werden, um die erforderliche Systemleistung sicherzustellen.

Vor Inbetriebnahme eines neuen Service/eines neuen Systems muss geprüft werden, ob die vorhandenen Kapazitäten auf FMG Seite (Netzwerk, IT-Personal, IT-Sicherheitssysteme) ausreichend dimensioniert sind, um den Betrieb sicherzustellen.

Für neue Services/neue Systeme muss die Möglichkeiten zur Kapazitätsüberwachung/-steuerung abgestimmt werden.

12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Maßnahme: Entwicklungs-, Test- und Betriebsumgebungen sollten voneinander getrennt sein, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.

Es ist eine Trennung in Form dedizierter Rollen oder Serversysteme zu gewährleisten.

12.2 Schutz vor Schadsoftware

Ziel: Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.

12.2.1 Maßnahmen gegen Schadsoftware

Maßnahme: Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer sollten umgesetzt werden.

BSIG-21: Jedes IT-System muss in geeigneter Weise vor Schadsoftware geschützt werden. Dabei müssen folgende Aspekte berücksichtigt werden:
a) Mehrstufiges Sicherheitskonzept (mindestens auf Netzwerk-, E-Mail- und Datei-Level)
b) Zentrales Management von Software durch eine definierte verantwortliche Einheit
c) Signatur- und verhaltensbasierte Erkennung von Schadsoftware
d) Zumindest tägliche Aktualisierung von der Virensignaturen
e) Prozesse zur Alarmierung von Anwendern und Administratoren bei Virenbefall
f) Protokollierung von Ereignissen in Bezug auf Schadsoftware
g) Umgang mit verschlüsselten Daten
Von der grundsätzlichen Implementierung kann unter folgenden Voraussetzungen abgewichen werden wenn:
a) der Hersteller des IT-Systems oder -Verbunds explizit den Einsatz einer Software zum Schutz vor Schadsoftware verbietet oder
b) der Einsatz der Software zum Schutz vor Schadsoftware drastische Performance-Einbußen bzw. Instabilitäten erzeugt oder
c) durch sonstige Maßnahmen sichergestellt ist, dass keinerlei Schadsoftware auf die Systeme ohne Schutz gelangen kann.
Die Software zum Schutz vor Schadsoftware muss regelmäßig, mindestens einmal täglich aktualisiert werden und folgende Merkmale aufweisen:
a) Prüfung aller Dateien, die auf elektronischen Medien bereitgestellt oder über Netze empfangen wurden;
b) Überprüfung von E-Mail-Anhängen und Downloads vor deren Verwendung;
Mindestens einmal pro Monat muss ein Komplett-Scan durchgeführt werden.
Es muss sichergestellt werden, dass durch infizierte Dateien kein weiterer Schaden verursacht werden kann (Löschen der Dateien; Verschieben in Quarantäne).

Der geeignete Schutz vor Schadsoftware muss auch virtuelle und Container-basierte Systeme umfassen.

Cloud-Dienste müssen durch den Cloud-Anbieter gegen Schadsoftware geschützt werden. Sollte der vom Cloud-Anbieter gestellte Schutz nicht ausreichend sein (z.B. durch fehlende Lizenzen), sind die nötigen Funktionen zu erwerben. Der Schutz vor Schadsoftware muss alle Dienste beinhalten, über die Daten ausgetauscht werden können.

12.3 Datensicherung

Ziel: Daten sind vor Verlust geschützt.

12.3.1 Sicherung von Information

Maßnahme: Sicherheitskopien von Information, Software und Systemabbildern sollten entsprechend einer vereinbarten Sicherungsrichtlinie angefertigt und regelmäßig getestet werden.

Es muss ein Datensicherungskonzept erarbeitet und umgesetzt werden, dass die Anforderungen der Geschäftsprozesse berücksichtigt.
Die Funktionsfähigkeit von Backup und Restore – einschließlich der Prüfung der Backup-Logs, regelmäßiger Restore-Tests – muss sichergestellt werden.
BSIG-24: Durchgeführte Restoretests müssen dokumentiert werden.
Vor Inbetriebnahme eines Systems muss mindestens ein Restoretest durchgeführt werden.

Eine Archivierung muss entsprechend der aktuell gültigen gesetzlichen Regelungen bzw. entsprechend den Anforderungen der Geschäftsprozesse durchgeführt werden.
Sämtliche relevanten Informationen müssen auf Basis der Verfügbarkeitsanforderungen gesichert werden.
Das angewandte Sicherungsverfahren muss für jedes IT-System dokumentiert werden. Die Dokumentation muss dabei Angaben zur Technik, zu Backupintervallen, zu Art und Umfang der Backups sowie zu Aufbewahrungszeiten der Backupmedien enthalten.
Jeder Backupvorgang muss überwacht und protokolliert werden. Die Protokolle müssen regelmäßig auf Vorhandensein und Vollständigkeit sowie hinsichtlich des Backupergebnisses überprüft werden.
Backups sind in regelmäßigen Abständen zu überprüfen. Hierzu zählen auch die Überprüfung des Inhalts der Backupmedien und die Wiederherstellung der Backupinformationen (Restore) auf einem geeigneten Prüfsystem.
Alle Backupmedien sind an einem sicheren und für die jeweiligen Medien geeigneten Ort, getrennt vom Betriebsort (unter Berücksichtigung von Brandschutzmaßnahmen), aufzubewahren. Bei Transport und Aufbewahrung sind die Backupmedien entsprechend des Schutzbedarfs der darauf gespeicherten Informationen in geeigneter Weise zu schützen.
BSIG-22: Der Zugriff auf Backups muss auf ein Mindestmaß beschränkt werden (ausschließlich autorisiertes Personal).

Vor dem Einsatz eines Cloud-Dienstes muss ein Backupkonzept für die darin gespeicherten Informationen erstellt werden. Dieses muss Backups außerhalb der Cloud bzw. bei einem anderen Cloud-Anbieter enthalten.

12.4 Protokollierung und Überwachung

Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.

12.4.1 Ereignisprotokollierung

Maßnahme: Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, sollten erzeugt, aufbewahrt und regelmäßig überprüft werden.

Die Aufbewahrungsdauer von Protokolldaten ist in Abstimmung mit dem Datenschutzbeauftragten und dem Betriebsrat festzulegen und sollte mindestens 12 Monate betragen.
Die nachfolgenden Aktivitäten und Transaktionen müssen protokolliert werden:

a) An- und Abmeldeversuche
b) Erstellung, Änderung oder Löschung von Benutzern und Erweiterung der Berechtigungen
c) Verwendung, Erweiterung und Änderungen von privilegierten Zugriffsberechtigungen
d) Nutzung von temporären Berechtigungen

Vertrauliche Daten, wie z. B. Passwörter, dürfen nicht protokolliert werden.
Es müssen Protokollierungsmechanismen für eigenen Code verwendet werden und die entsprechenden Funktionen der Produkte, die eingesetzt werden (Web-Server, Anwendungsserver, Datenbank, Betriebssystem usw.) müssen aktiviert werden.
Interne Systemmeldungen (Log-Files) müssen auf erkennbare Missbrauchsversuche (z. B. Passwortraten) überwacht werden.

BSIG-80/91: Protokolldaten müssen zentral aggregiert und konsolidiert werden. Es muss regelmäßig überprüft werden

- ob alle kritischen IT-Systeme (IT-Systeme, OT-Systeme, Applikationen, IoT-Geräte, Endgeräte, ...) an die zentrale Log-Infrastruktur angebunden sind und falls erforderlich angebunden werden
- ob die geloggten Use-Cases für bereits angebundene IT-Systeme noch aktuell sind, oder ggf. angepasst werden müssen.

CV: An das SIEM angebundene Systeme müssen die produzierten Log-Files kontinuierlich (zumindest aber tagesaktuell) an das SIEM weiterleiten. Es müssen Verfahren etabliert werden, sodass der unberechtigte/unautorisierte Abfluss von Firmendaten- bzw. Informationen frühzeitig erkannt und wird und unterbunden werden kann.

Der Cloud-Anbieter muss die Möglichkeiten zur Protokollierung in der Umgebung oder der jeweiligen Dienste aufzeigen. Hierbei müssen mindestens die genutzten Dienste, Formate zur Datenübertragung und Schnittstellen sowie die Möglichkeiten zur Umsetzung FMG eigener Lösungen berücksichtigt werden.

Es muss sichergestellt werden, dass die möglichen und notwendigen Protokollierungs-Funktionen in einem Cloud-Dienst aktiviert sind.

12.4.2 Schutz der Protokollinformation

Maßnahme: Protokollierungseinrichtungen und Protokollinformation sollten vor Manipulation und unbefugtem Zugriff geschützt sein.

BSIG-93: Zum Schutz der Sicherheit der aufgezeichneten Protokolldaten muss folgendes umgesetzt werden:
- Verfügbarkeit: Sicherstellung von ausreichemden Speicherplatz (sodass Log-Daten nicht überschrieben werden bzw. dadurch verloren gehen)
- Integrität: Sicherstellung, dass Log-Files nicht (absichtlich oder unabsichtlich) manipuliert werden können (Zugriffschutz, Weiterleitung an einen Zentralen Log-Host, ...)
- Vertraulichkeit: Sicherstellung, dass die Log-Files nur von autorisiertem Personal eingesehen bzw. Analysiert werden kann (Zugriffschutz)

12.4.3 Administratoren- und Bedienerprotokolle

Maßnahme: Tätigkeiten von Systemadministratoren und Systembedienern sollten aufgezeichnet und die Protokolle sollten geschützt und regelmäßig überprüft werden.

BSIG/CV: Aktionen, die mittels privilegierten Accounts (z.B. Admin-Accounts, Service-Accounts) durchgeführt werden müssen protokolliert und regelmäßig kontrolliert werden.
Die Überwachung muss mindestens die nachfolgenden Ereignisse umfassen:
a) genehmigter Zugang
b) alle privilegierten Operationen
c) unbefugte Zugriffsversuche
d) Systemalarme und Fehler
e) Änderungen oder der Versuch von Änderungen an den Sicherheitseinstellungen des Systems oder an dessen Sicherheitsmaßnahmen.

12.4.4 Uhrensynchronisation

Maßnahme: Die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder eines Sicherheitsbereichs sollten mit einer einzigen Referenzzeitquelle synchronisiert sein.

Beim Einsatz eines Cloud-Dienstes sollte eine gemeinsame Zeit-Quelle zum Einsatz kommen oder die Möglichkeit zur Zeit-Synchronisation mit lokalen Systemen der FMG oder anderen Cloud-Diensten geprüft werden.

12.5 Steuerung von Software im Betrieb

Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.

12.5.1 Installation von Software auf Systemen im Betrieb

Maßnahme: Verfahren zur Steuerung der Installation von Software auf Systemen im Betrieb sollten umgesetzt werden.

BSIG-25/CV: Vor Inbetriebnahme einer Anwendung, eines IT-Systems, eines OT-Systems, eines Endgeräts oder eines IoT-Geräts müssen Härtungsmaßnahmen durchgeführt werden, die insbesondere folgende Punkte beinhalten:

a) die Deaktivierung sämtlicher nicht erforderlicher Dienste, Schnittstellen und Ports,
b) die Deaktivierung oder Deinstallation sämtlicher nicht erforderlicher Anwendungen sowie
c) die Berücksichtigung von herstellerspezifischen Hinweisen bzw. anerkannte Industriestandards zur sicheren Konfiguration der Anwendungen und Systeme.

Die verwendeten Härtungsanleitungen und der Umsetzungsstatus der Härtungsmaßnahmen müssen dokumentiert werden.
Anwendungen und Betriebssystemsoftware sollten nur nach ausgiebigen und erfolgreichen Tests eingespielt werden. Die Tests sollten Benutzbarkeit, Sicherheit, Nebenwirkungen auf andere Systeme beinhalten und auf separaten Systemen (siehe auch 14.2.8) durchgeführt werden.

Für alle eingekauften Cloud-Dienste muss eine Härtung der Konfiguration vorgenommen werden. Hierbei sind die Vorgaben der Anbieter und anerkannte Industriestandards zu beachten. Hierbei sind Abhängigkeiten zwischen den Diensten zu berücksichtigen. Die Cloud-Umgebung (auch Cloud-Tenant oder –Konto genannt) sollte möglichst automatisiert abgesichert werden.

Diese sichere Konfiguration muss regelmäßig überprüft werden und ggf. an neue Funktionen angepasst werden. Hierbei sind die Intervalle vom Cloud-Dienst abhängig. Bei vielen Änderungen sollte eine wöchentliche oder monatliche Überprüfung stattfinden. Die Prüfung muss jedoch mindestens jährlich erfolgen.

12.6 Handhabung technischer Schwachstellen

Ziel: Die Ausnutzung technischer Schwachstellen ist verhindert.

12.6.1 Handhabung von technischen Schwachstellen

Maßnahme: Informationen über technische Schwachstellen verwendeter Informationssysteme sollte rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen sollte bewertet und angemessene Maßnahmen ergriffen werden, um das dazugehörige Risiko zu behandeln.

CV: Schwachstellen in IT-Systemen und Applikationen (einschließlich Webanwendungen) müssen regelmäßig (mind. monatlich) identifiziert werden. Kritische Schwachstellen müssen zeitnah (= spätestens innerhalb von 15 Tagen) beseitigt werden.

Ein wirksamer Patch-Prozess, der mindestens die nachfolgenden Aspekte enthält muss etabliert sein:

a) Regelmäßige Identifikation und Analyse (= mindestens monatlich) der IT-Systeme auf vorhandene Schwachstellen (z.B. fehlende Security-Patches, ...)
b) Definition von Verantwortlichkeiten für die Überwachung und Risikobewertung von Schwachstellen sowie die Durchführung und Prüfung von Aktualisierungen

c) Patches sind vor dem Rollout auf Funktionsfähigkeit und Wechselwirkungen mit relevanten Anwendungen und Systemen zu testen.
d) Patches sind in Abhängigkeit der Kritikalität des Patches und der betroffenen Systeme (Vertraulichkeits-, Integritäts- sowie Verfügbarkeitsanforderungen) zeitnah zu installieren.
e) Der aktuelle Patch-Level sowie fehlende Patches müssen zu jeder Zeit für jedes System nachvollziehbar sein.

Ports, Dienste und ähnliche Einrichtungen, die auf einem Computer oder in einer anderen Komponente vorhanden und für den Betrieb nicht unbedingt erforderlich sind, müssen deaktiviert, entfernt oder anderweitig geschützt werden.

12.6.2 Einschränkungen von Softwareinstallation

Maßnahme: Regeln für die Softwareinstallation durch Benutzer sollten festgelegt und umgesetzt werden.

12.7 Audits von Informationssystemen

Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.

12.7.1 Maßnahmen für Audits von Informationssystemen

Maßnahme: Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systeme beinhalten, sollten sorgfältig geplant und vereinbart werden, um Störungen der Geschäftsprozesse zu minimieren.

Auditaktivitäten (Security Review, Penetrationstests, Schwachstellenscans, ...) müssen so durchgeführt werde, dass keine Auswirkungen auf den Geschäftsbetrieb entstehen (z.B. Definition von abgestimmten Zeitfenstern in denen die Audits durchgeführt werden, Durchführung auf dezidierten Testumgebungen, Wahl einer angemessenen Audit-intensität, ...).

Die IT-Sicherheit der genutzten Cloud-Dienste sollte nach Möglichkeit über automatische Funktionen überprüft werden. Bei der Planung sollte das CDC des Anbieters oder der ISEC-Beauftragte der FMG einbezogen werden.

12.7.2 Penetrationsprüfungen von Anwendungen

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

CV: Penetrationstests müssen regelmäßig (= mind. quartalsweise) durchgeführt werden. Dies gilt u.a. für, wichtige / kritische Anwendungen, Web-Anwendungen, IT-Systeme, IoT-Systeme, ICS-Systeme, Server, Cloud-Systeme, Infrastruktur und alle wichtigen Endbenutzersystems (FMG-Standard Client).

Bei der Nutzung von Cloud-Diensten (insbesondere SaaS und PaaS) sollten zusätzlich zu den geplanten Penetrationstest kontinuierliche Audits implementiert werden. Dies kann auf Basis von automatischen Sicherheitsscannern (Schwachstellenscans) durch den Cloud Anbieter-erfolgen. Sollte dies nicht möglich sein, so sollte dies quartalsweise durch die FMG erfolgen.

Luftverkehrsspezifische Umsetzungsvorgaben (gem. CoPiP 3.2)

Regelmäßige Penetrationsprüfungen von Anwendungen sollten bei geschäftskritischen Anwendungen jedes Jahr festgelegt sein. Außerdem sollten Penetrationsprüfungen regelmäßig (d.h. mindestens jährlich) sowie 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 falschpositive und falschnegative 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 intelligenten 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.

12.7.3 Penetrationsprüfungen von Infrastrukturen

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

CV: Es müssen regelmäßig simulierte (Distributed) Denial of Service (D)DoS-Angriffe durchgeführt werden um etablierte Maßnahmen zur Verhinderung von DDoS-Angriffen zu verifizieren.

Beim Einsatz von IaaS Diensten sollten zusätzlich zu den geplanten Penetrationstest kontinuierliche Audits implementiert werden. Dies kann auf Basis von automatischen Sicherheitsscannern (Schwachstellenscans) durch den Cloud-Anbieter erfolgen. Sollte dies nicht möglich sein, so sollte dies quartalsweise durch die FMG erfolgen.

Luftverkehrsspezifische Umsetzungsvorgaben (gem. CoPiP 3.2)

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 falschpositive und falschnegative 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 intelligenten 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 Kommunikationssicherheit

13.1 Netzwerksicherheitsmanagement

Ziel: Der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt.

13.1.1 Netzwerksteuerungsmaßnahmen

Maßnahme: Netzwerke sollten verwaltet und gesteuert werden, um Information in Systemen und Anwendungen zu schützen.

Öffentlich zugängliche Systeme müssen mit Sicherheitsmechanismen ausgestattet werden, die eine Verbindung nur zu erlaubten Systemen zulassen.
BSIG-37: Eine angemessene Protokollierung und Überwachung zur Erkennung von Anomalien (z.B. MAC-Spoofing, ARP-Poisoning, DDoS, ...) muss angewandt werden. Verbindungen zwischen vertrauenswürdigen und nicht-vertrauenswürdigen Netzen müssen überwacht werden.
Fremdsysteme dürfen nur über entsprechende Schutzmechanismen (Firewall, Proxy etc.) an die IT-Systeme des FMG-Konzerns angeschlossen werden.
BSIG-38: Jedes Netzwerkperimeter muss über Sicherheitsgateways kontrolliert werden.
Ausnahmen dürfen vom Betreiber des internen Netzes nur genehmigt werden, wenn sichergestellt ist, dass diese Systeme vor Verbindungsaufbau umfassend und aktuell auf Viren und bösartige oder nicht erwünschte Anwendungen überprüft werden und somit keine Gefährdungen für die IT-Systeme des FMG-Konzerns darstellen. Eine Prüfung kann erfolgen durch
a) den Betreiber des internen Netzes
b) den Bediener des Fremdsystems, sofern vom Eigentümer vertraglich zugesichert ist, dass das System ISEC-Richtlinien-konform betrieben wird

Ausnahmen dürfen vom Betreiber des internen Netzes nur genehmigt werden, wenn sichergestellt ist, dass diese Systeme vor Verbindungsaufbau umfassend und aktuell auf Viren und bösartige oder nicht erwünschte Anwendungen überprüft werden und somit keine Gefährdungen für die IT-Systeme des FMG-Konzerns darstellen. Eine Prüfung kann erfolgen durch
a) den Betreiber des internen Netzes
b) den Bediener des Fremdsystems, sofern vom Eigentümer vertraglich zugesichert ist, dass das System ISEC-Richtlinien-konform betrieben wird

Alle relevanten Informationen (z. B. Netzwerkpläne, IP-Adressbereiche) zu den bei bzw. explizit für den FMG-Konzern betriebenen Netzwerken sind in einem zentralen Bestandsverzeichnis zu pflegen.
Bei der Planung und Umsetzung von Maßnahmen für Netzwerke sind die Anforderungen
a) an die Verfügbarkeit,
b) an Vertraulichkeit und Integrität (insbesondere bei Informationsaustausch über öffentliche Netzwerke)
zu berücksichtigen.

In festgelegten Abständen wird die geschäftliche Rechtfertigung für die Verwendung aller Dienste, Protokolle und Ports überprüft. Darüber hinaus umfasst die Überprüfung auch die Begründungen für kompensierende Kontrollen für die Verwendung von Protokollen, die als unsicher angesehen werden.

BSIG-40: Die Architektur des Netzwerks muss nachvollziehbar und aktuell dokumentiert werden (= Netzplan).

CV: Der Zugriff auf das Firmennetzwerk durch unbekannte bzw. unautorisierte Endgeräte (via WLAN oder anstecken an LAN-Port) muss unterbunden werden. Dies sollte durch Implementierung von Port-Security (z.B. MAC-Filtering, NAC, 802-1x) umgesetzt werden. Neue, bzw. unbekannte oder unautorisierte Endgeräte im Firmennetz müssen protokolliert bzw. identifiziert und an das CDC weitergeleitet werden.

13.1.2 Sicherheit von Netzwerkdiensten

Maßnahme: Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste sollten bestimmt und sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufgenommen werden.

Informationen über Netzwerkdesign und Maßnahmen zum Schutz von Netzdiensten sind mindestens als „Vertraulich" einzustufen und in entsprechender Weise zu schützen.
Das FMG-Konzern-System ist regelmäßig auf nicht autorisierte verbundene Netzwerke (z. B. nicht von IT bereitgestellte WLANs) zu überprüfen und diese ggf. außer Betrieb zu nehmen.
Systeme oder Netze, die für Remote-Zugriffe genutzt werden, müssen gegen unbefugten Zugriff geschützt werden. Sie müssen mit einer sicheren Konfiguration inkl. Virenschutz und sicherer Authentifizierung ausgerüstet werden.
Remote-Zugriffsverbindungen müssen von Produktionsnetzwerken durch Firewall-Mechanismen getrennt werden.
Remote-Zugriffe über öffentliche Netze (z. B. Internet) müssen durch den Einsatz eines verschlüsselten VPNs abgesichert werden. Bei einer ISDN-Verbindung mit vordefiniertem Rückruf (predefinied callback) oder einer Verbindung über eine private Standleitung (ISDN, ATM) ist keine VPN-Verschlüsselung notwendig.
Remote-Zugriffe über Transfernetze müssen generell verschlüsselt werden, es sei denn, der Betreiber des Fremd-Netzwerkes betreibt dieses konform zu den Anforderungen dieser Richtlinie.
Die Verbindungsdaten von Remote-Zugriffssitzungen müssen protokolliert werden.
Die Remote-Zugriffsysteme und das Netz, in dem sie sich befinden, müssen in Übereinstimmung mit den Anforderungen dieses Standards betrieben werden.
Der Zugriff auf Remote-Services bzw. Remote-Anmeldungen, sowie alle extern erreichbaren (= internet-facing) IT-Systeme müssen durch MFA geschützt werden. Ausgenommen hiervon ist ein Zugriff auf:

- von der FMG bereitgestellte bzw. im Auftrag der FMG betriebene Webservices,
- Geschäftsinformationen über öffentliche Netze von mobilen Geräten, sofern hierfür eine Identifikation und Authentisierung unter Anwendung angemessener Zugangskontrollmechanismen erforderlich ist.

Es müssen mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführt werden. Die Penetrationstests erfolgen nach einer dokumentierten Testmethodik und umfassen die für den sicheren Betrieb der kritischen Dienstleistung als kritisch definierte Infrastruktur-Komponenten, die im Rahmen einer Risiko-Analyse als solche identifiziert wurden. Art, Umfang Zeitpunkt/Zeitraum und Ergebnisse werden für einen sachverständigen Dritten nachvollziehbar dokumentiert. Feststellungen aus den Penetrationstests werden bewertet und mindestens bei mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit der kritischen Dienstleistung nachverfolgt und behoben. Die Einschätzung der Kritikalität und der mitigierenden Maßnahmen zu den einzelnen Feststellungen werden dokumentiert.

CV: kritische Serverkommunikation muss verschlüsselt werden.

Es sollten nur Protokolle genutzt werden, welche sich mit gängigen Sicherheitstools überwachen lassen. Sollte dies nicht möglich sein (z.B. bei Websockets) so sind diese Protokolle genau zu beschreiben (ggf. durch den Anbieter selber). Hierbei dürfen nur Signalisierungen (z.B. über eine neue Nachricht) über das Websocket Protokoll erfolgen. Jedwede weitere Kommunikation muss über ein gesichertes HTTPS Protokoll erfolgen.

13.1.3 Trennung in Netzwerken

Maßnahme: Informationsdienste, Benutzer und Informationssysteme sollten in Netzwerken gruppenweise voneinander getrennt gehalten werden.

a) Alle Verbindungen zwischen dem internen Netzwerk des FMG-Konzerns und externen Netzwerken (z. B. dem Internet und Netzwerken von Lieferanten oder Partnern des FMG-Konzerns) müssen durch technische Maßnahmen (z. B. Firewall) und Zugriffskontrollmechanismen gesichert werden.
b) Zugänge zu FMG-Konzern-Netzwerken (z. B. Netzwerkdosen, Netzwerkkabel) in physisch öffentlich zugänglichen Bereichen müssen vermieden werden. Sofern erforderlich müssen diese durch geeignete physische (z. B. Absperren) oder logische (z. B. ACL, Netzwerkzugangskontrollsysteme) Sicherheitsmaßnahmen vor unberechtigter Nutzung geschützt werden.
c) Drahtlose Netze müssen von internen und privaten Netzen getrennt werden, falls keine starke Authentifizierung wie beispielsweise WPA2 beim Zugriff auf das Netzwerk stattfindet.
d) BSIG-39: Netzwerke zur Verwaltung der Infrastruktur und für den Betrieb von Managementkonsolen müssen (logisch oder physisch) getrennt werden und dessen Zugriff muss zusätzlich über Multi-Faktor-Authentisierung geschützt werden.
e) CV: Das Firewall-Regelwerk muss regelmäßig (= mindestens monatlich) überprüft und bei Bedarf müssen nicht (mehr) benötigte oder zu weitreichende Firewallregeln entfernt, deaktiviert oder angepasst werden.

Die Vertrauenswürdigkeit für Cloud-Dienste und virtuelle Netzwerke in Cloud-Diensten muss festgelegt werden. Hierbei muss definiert werden, welche FMG Zonen auf den Cloud-Dienst zugreifen können und es hierbei zu keiner Kopplung verschiedener Zonen kommt. Für eine vollständige Betrachtung müssen alle Komponenten und Netze betrachtet werden (z.B. FMG Netze, das Internet, FMG gemanagte Geräte, Dienstleister, sonstige nicht verwaltete Geräte, Mobilgeräte und sonstige öffentliche Netze).

Darüber hinaus muss berücksichtigt werden, dass eine Separierung produktiver Netzwerke sowie Management- und Administrationsnetze eingehalten werden sollte.

13.2 Informationsübertragung

Ziel: Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, ist aufrechterhalten.

13.2.1 Richtlinien und Verfahren für die Informationsübertragung

Maßnahme: Formale Übertragungsrichtlinien, -verfahren und -maßnahmen sollten vorhanden sein, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen.

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „IT-Nutzungsrichtlinie“ eingehalten werden.

13.2.2 Vereinbarungen zur Informationsübertragung

Maßnahme: Vereinbarungen sollten die sichere Übertragung von Geschäftsinformationen zwischen der Organisation und externen Parteien behandeln.

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „IT-Nutzungsrichtlinie" eingehalten werden.

13.2.3 Elektronische Nachrichtenübermittlung

Maßnahme: Information in der elektronischen Nachrichtenübermittlung sollte angemessen geschützt sein.

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern von ihm beauftragten Dienstleistern die „IT-Nutzungsrichtlinie" eingehalten werden.

13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Maßnahme: Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, sollten identifiziert, regelmäßig überprüft und dokumentiert werden.

a) In einem direkten Auftraggeber-/Auftragnehmerverhältnis muss die FMG-Konzern-spezifische Vertraulichkeitsvereinbarung verwendet werden.
b) Zwischen Auftraggeber und Auftragnehmer muss eine Vertraulichkeitsvereinbarung vorliegen. Diese muss vor Vergabe des Zugriffs von der verpflichteten Partei unterzeichnet werden.
c) Anpassungen bzw. fremde Vertraulichkeitsvereinbarungen müssen durch die Rechtsabteilung des FMG-Konzerns freigegeben werden.
d) **BSIG-42**: Abgeschlossene Vertraulichkeits- oder Geheimhaltungsvereinbarungen müssen mindestens jährlich überprüft und bei Bedarf angepasst werden.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen an Informationssysteme

Ziel: Es ist sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.

14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Maßnahme: Die Anforderungen, die sich auf Informationssicherheit beziehen, sollten in die Anforderungen an neue Informationssysteme oder die Verbesserungen bestehender Informationssysteme aufgenommen werden.

Bei der Definition von Sicherheitsanforderungen sind folgende Punkte zu berücksichtigen:
a) Durchführung einer frühzeitigen Schutzbedarfsanalyse der betroffenen Systeme/Informationen,
b) Durchführung einer Gefährdungsanalyse mit Bedrohungen und Schwachstellen,
c) Definition und Abfrage von Sicherheitsanforderungen an den möglichen Lieferanten sowie das zu beauftragende System im Rahmen der Auftragsbeschreibung,

d] Erstellung eines Sicherheitskonzeptes für Systeme mit hohem oder sehr hohem Schutzbedarf.
e] Die Verpflichtung zur Durchführung eines Vulnerability Scans mit definiertem Umfang/Scope vor Inbetriebnahme von Systemen und Anwendungen, die aus dem Internet erreichbar sind.
f] Die Freigabe neuer Systeme muss durch das Management erfolgen.
g] Das Management muss festlegen, in welchem Rahmen die Wartung und Erfüllung der Sicherheitsanforderungen erfolgt und wer für diese verantwortlich ist.

Luftverkehrsspezifische Umsetzungsvorgaben

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

14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken

Maßnahme: Information, die durch Anwendungsdienste über öffentliche Netzwerke übertragen wird, sollte vor betrügerischer Tätigkeit, Vertragsstreitigkeiten und unbefugter
Offenlegung sowie Veränderung geschützt werden.

Ein Sicherheitskonzept für E-Commerce-Anwendungen muss erstellt werden. Dieses muss mindestens die folgenden Punkte enthalten:
a] Eindeutige Authentisierung der relevanten Parteien
b] die Sicherstellung der Vertraulichkeit, Integrität sowie der Nichtabstreitbarkeit jeglicher Bestelltransaktion, Zahlungsinformation, Lieferadresse sowie der Bestätigung von Rechnungen
c] Die Aufrufbarkeit der Geschäftsbedingungen bei Vertragsabschluss.
Bei Systemen, die Kreditkartendaten speichern, sind zwingend die Vorgaben des PCI DSS einzuhalten.
Bevor Informationen öffentlich bereitgestellt werden, muss deren Veröffentlichung durch den Informationsverantwortlichen genehmigt werden.
Die Integrität öffentlich zugänglicher Informationen muss durch geeignete Maßnahmen (z. B. Absicherung von Webservern und Applikationen) gegen unberechtigte Veränderungen geschützt werden.
Das öffentlich zugängliche System ist auf Schwachstellen und Fehler zu untersuchen, bevor dort Informationen bereitgestellt werden.
Es ist sicherzustellen, dass der Zugriff auf das Veröffentlichungssystem keinen unbeabsichtigten bzw. unerlaubten Zugriff auf Netze ermöglicht, die an das System angeschlossen sind.

14.1.3 Schutz der Transaktionen bei Anwendungsdiensten

Maßnahme: Information, die an Transaktionen bei Anwendungsdiensten beteiligt ist, sollte so geschützt werden, dass unvollständige Übertragung, Fehlleitung, unbefugte Offenlegungen, unbefugte Vervielfältigungen oder unbefugte Wiederholung von Nachrichten verhindert ist.

14.1.4 Richtlinie für Webanwendungen/Web-Services

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

Die folgenden Regelungen für Genehmigungsverfahren bei neuen informationsverarbeitenden Einrichtungen (insbesondere neue Technologien) müssen betrachtet werden:
a] Die Freigabe neuer Systeme muss durch das Management erfolgen.
b] Das Management muss festlegen, in welchem Rahmen die Wartung und Erfüllung der Sicherheitsanforderungen erfolgt und wer für diese verantwortlich ist.

Luftverkehrsspezifische Umsetzungsvorgaben

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

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Ziel: Es ist sichergestellt, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist.

14.2.1 Richtlinie für sichere Entwicklung

Maßnahme: Regeln für die Entwicklung von Software und Systemen sollten festgelegt und bei Entwicklungen innerhalb der Organisation angewendet werden.

BSIG-43: Die Einführung von neuen Systemen muss einem formalen Prozess (= Secure Development Lifecycle) folgen. Dieser Prozess sollte gängigen Best Practices oder Standards in der jeweiligen Entwicklungsumgebung und -sprache (OWASP, SAFEcode, ISO 27035, ...) folgen bzw. müssen die Entwicklungsaktivitäten einem gleichwertigem Sicherheitsniveau entsprechen.

14.2.2 Verfahren zur Verwaltung von Systemänderungen

Maßnahme: Änderungen an Systemen innerhalb des Entwicklungszyklus sollten durch formale Verfahren zur Verwaltung von Änderungen gesteuert werden.

Die Einführung von neuen Systemen und größeren Änderungen an bestehenden Systemen muss einem formalen Prozess folgen, der zumindest folgende Punkte berücksichtigt:

a) Risikobetrachtung der Systemänderung
b) Ermittlung der Auswirkungen inkl. Durchführung der mit der Änderung verbundenen erforderlichen Aktivitäten (z.B. zusätzliche Tests, Anpassung der Dokumentation, ...)
c) Dokumentation der Testergebnisse
d) Einhaltung der definierten Freigabeprozeduren
e) Änderungen dürfen nur von autorisierten Nutzern durchgeführt werden, Änderungen durch nicht-Autorisierte müssen verhindert werden.
f) Bei wesentlichen Änderungen muss die Möglichkeit zum Rollback auf den vorherigen Zustand gegeben sein.
g) Es muss sichergestellt sein, dass die Implementierung von Änderungen zu einem mit den betroffenen Bereichen abgestimmten Zeitpunkt erfolgt.

14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform

Maßnahme: Bei Änderungen an Betriebsplattformen sollten geschäftskritische Anwendungen überprüft und getestet werden, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder Organisationssicherheit gibt.

Es ist sicherzustellen, dass relevante Änderungen auch in den Business-Continuity-Plänen (siehe Abschnitt 17) berücksichtigt werden.

14.2.4 Beschränkung von Änderungen an Softwarepaketen

Maßnahme: Änderungen an Softwarepaketen sollten nicht gefördert werden, auf das Erforderliche beschränkt sein, und alle Änderungen sollten einer strikten Steuerung unterliegen.

14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme

Maßnahme: Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sollten festgelegt, dokumentiert, aktuell gehalten und bei jedem Umsetzungsvorhaben eines Informationssystems angewendet werden.

- Benutzer dürfen nur die absolut notwendigen technischen Informationen in der Fehlermeldung erhalten. Inkonsistenzen, die zur unbeabsichtigten Offenlegung von Informationen führen oder Angriffe begünstigen könnten, sind durch das Abdecken
  aller Ausnahmen, die in der Anwendung bzw. dem Framework und den APIs (Application Programming Interfaces) vorkommen, zu vermeiden.
- Ausführliche Fehlermeldungen sind im Fehlerprotokoll festzuhalten und müssen eine Fehler-ID enthalten. Mit dieser Fehler-ID kann eine Fehlermeldung, welche dem Benutzer angezeigt wird, die detaillierte (technische) Fehlermeldung referenzieren.
- Die Behandlung und Verbreitung von Fehlern und Ausnahmen innerhalb der Anwendung ist sorgfältig zu planen.
- Bei der Planung und Realisierung von Anwendungen und Systemen muss berücksichtigt werden, dass diese keine vertraulichen Daten preisgeben, die einem Angreifer eventuelle Schwachstellen in der Anwendung aufzeigen (z. B. detaillierte Versionsnummern, Patchstände etc.).

14.2.6 Sichere Entwicklungsumgebung

Maßnahme: Organisationen sollten sichere Entwicklungsumgebungen für Systementwicklungs- und Systemintegrationsvorhaben über den gesamten Entwicklungszyklus schaffen und diese angemessen schützen.

14.2.7 Ausgegliederte Entwicklung

Maßnahme: Die Organisation sollte die Tätigkeit ausgegliederter Systementwicklung beaufsichtigen und überwachen.

BSIG-44: Bei Auslagerung von Entwicklungsaktivitäten müssen vom Entwicklungsdienstleister Nachweise eingefordert werden, dass dieser Software bzw. Applikationen gem. Stand-der-Technik bzw. nach anerkannten Standards und Best Practices entwickelt. Des Weiteren muss für Entwicklungsdienstleister ein Recht zur Auditierung der Entwicklungsprozesse vertraglich vereinbart werden.

14.2.8 Testen der Systemsicherheit

Maßnahme: Die Sicherheitsfunktionalität sollte während der Entwicklung getestet werden.

14.2.9 Systemabnahmetest

Maßnahme: Für neue Informationssysteme, Aktualisierungen und neue Versionen sollten Abnahmetestprogramme und dazugehörige Kriterien festgelegt werden.

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.

14.2.10 Entwicklung von Anwendungen

Maßnahme: Für Webanwendungen sollten sichere Entwicklungsrichtlinien angewendet werden.

Luftverkehrsspezifische Umsetzungsvorgaben

Die folgenden Schlüsselbereiche bei der Entwicklung von Webanwendungen sollten abgedeckt sein:
- 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.

14.2.11 Code-Reviews

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

Luftverkehrsspezifische Umsetzungsvorgaben

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.

CV: Code Reviews müssen für alle selbstentwickelten und zugekauften Webanwendungen durchgeführt werden.

14.3 Testdaten

Ziel: Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.

14.3.1 Schutz von Testdaten

Maßnahme: Testdaten sollten sorgfältig ausgewählt, geschützt und gesteuert werden.

Produktivdaten oder Teile von Produktivdaten, die zu Testzwecken genutzt werden müssen, müssen grundsätzlich durch geeignete Verfahren (z. B. Scrambling, Pseudonymisierung) verfremdet werden. Sofern dies nicht möglich ist, sind Maßnahmen zum Schutz dieser Daten in Abhängigkeit ihrer Vertraulichkeit zu gewährleisten.

15 Lieferantenbeziehungen

15.1 Informationssicherheit in Lieferantenbeziehungen

Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.

15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen

Maßnahme: Die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation müssen mit dem Zulieferer vereinbart und dokumentiert werden.

Bei bereichsübergreifenden Geschäftsprozessen, sowie bei Beauftragung von Dienstleister oder Lieferanten muss vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Werte (Services, Systeme etc.) festgelegt werden (Beispieltabelle zur Zuordnung von Mindestverantwortlichkeiten siehe Anhang 1).

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 (siehe Abschnitt 8) festgelegt werden.

15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

Maßnahme: Alle relevanten Informationssicherheitsanforderungen sollten mit jedem Lieferanten, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt, festgelegt werden und vereinbart sein.

BSIG-98:
Vor Beauftragung eines Lieferanten bzw. Dienstleisters muss dieser vor Aufnahme der Tätigkeit angemessen auf die Einhaltung der relevanten FMG Informationssicherheitsvorschriften verpflichtet werden, d.h.
a) Unterzeichnung einer Vertraulichkeitsvereinbarung (NDA), vor Vergabe der Zugriffsberechtigung

b) Verpflichtung zur Einhaltung der für die Aufgabenerfüllung relevanten FMG-Richtlinien (durch einen zeichnungsberechtigten Vertreter der externen Firma) und die Verpflichtung zur Weitergabe der Verpflichtung an alle für FMG tätigen Mitarbeiter und beauftragte Dienstleister beinhalten.
c) Bei der Definition von Sicherheitsanforderungen ist die ISEC-Richtlinie BE in der jeweils gültigen Fassung zu verwenden.
d) Es ist sicherzustellen, dass zu jedem Zeitpunkt der Zusammenarbeit mit Lieferanten Sicherheitsaspekte definiert und verbindlich vereinbart sind.
e) Dies beinhaltet insbesondere:
   - die Verpflichtung des Lieferanten zur Information aller an der Auftragserfüllung beteiligten Personen über einzuhaltende Verpflichtungen/Sicherheitsaspekte,
   - die Verpflichtung zur Meldung sämtlicher Ereignisse mit möglichen sicherheitsrelevanten Auswirkungen auf den Auftraggeber,
   - die Verpflichtung des Lieferanten, die Einhaltung aller an ihn gestellten Sicherheitsanforderungen gegenüber Subunternehmen und Erfüllungsgehilfen sicherzustellen sowie
   - die Vereinbarung des Rechts zur Prüfung von Sicherheitsanforderungen (Auditrecht)

Vor Nutzung eines Cloud-Dienstes muss die angemessene und wirksame Umsetzung der Basisanforderungen nach BSI C5 oder ISO 27001 erfolgen. Hierbei sind zertifizierte Cloud Anbieter zu bevorzugen. Der Scope und das Statement of Applicability auf dem Zertifikat müssen den geforderten Leistungsumfang abdecken. Sollte kein Zertifikat vorliegen, kann alternativ durch ein Audit von FMG ISM auf Basis der FMG IS-Standards erfolgen sofern dies von ISM gewünscht ist.

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Maßnahme: Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, sollten in Vereinbarungen mit Lieferanten aufgenommen werden.

Die Beteiligung von Unterauftragnehmern und anderen externen Dritten müssen vom Cloud-Anbieter vollständig in Art und Umfang benannt werden. Beabsichtigte Änderungen hierüber müssen unverzüglich schriftlich oder per E-Mail mitgeteilt werden. Diese Mitteilungen können auch über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

Falls Unterauftragnehmer nicht nur unwesentliche Teile zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, muss der Cloud-Anbieter zusichern, dass Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und dass zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

15.2 Steuerung der Dienstleistungserbringung von Lieferanten

Ziel: Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im Einklang mit Lieferantenverträgen aufrechterhalten.

15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen

Maßnahme: Organisationen sollten die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, überprüfen und auditieren.

Die Erfordernis sowie Art und Umfang von Überprüfungen der bei Lieferanten umgesetzten Sicherheitsmaßnahmen sind für die erteilten Aufträge festzulegen. Die Durchführung ist durch geeignete Personen vorzunehmen und zu dokumentieren.
Die Überwachung- bzw. Überprüfung der Leistungserbringung des Lieferanten sollte folgendes beinhalten:

- Regelmäßige Kontrolle von Dienstleistungsberichten (z.B. SLA-Reporting)
- Überprüfung von sicherheitsrelevanten Vorfällen, Störungen, Ausfällen und Unterbrechungen, die mit der für die FMG erbrachte Dienstleistung verbunden sind.
- Regelmäßige bzw. außerplanmäßige Überprüfungen, z.B.: bei wesentlichen Änderungen
- Durchführung einer Risikoanalyse und Definition erforderlicher Maßnahmen bei Feststellung von Abweichungen bzw. nicht-Einhaltung von Sicherheitsvorschriften der FMG durch den Lieferanten.

Die Zertifikate nach C5 oder ISO 27001 müssen jährlich durch die FMG überprüft werden. Alternativ kann je nach Risikoeinstufung des Cloud-Dienstes bzw. des Cloud-Anbieters ein Audit durch den ISEC-Beauftragten erfolgen.

15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen

Maßnahme: Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten sollten gesteuert werden. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -verfahren und -maßnahmen. Dabei sollten die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet werden.

16 Handhabung von Informationssicherheitsvorfällen

16.1 Handhabung von Informationssicherheitsvorfällen und –verbesserungen

Ziel: Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.

16.1.1 Verantwortlichkeiten und Verfahren

Maßnahme: Handhabungsverantwortlichkeiten und -verfahren sollten festgelegt werden, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle sicherzustellen.

Sicherheitsrelevante Vorfälle müssen analysiert und bewertet werden. Wenn im Rahmen der Bewertung Handlungsbedarf ermittelt wird, müssen entsprechende Maßnahmen ergriffen werden.
BSIG-71: Es muss sichergestellt, dass für Sicherheitsvorfälle ein dokumentierter Prozess inkl. Verantwortlichkeiten existiert, d.h. es in jedem Bereich geprüft werden, ob zentrale Vorgaben anwendbar bzw. sinnvoll sind. Falls nicht muss im jeweiligen Bereich ein dezidierter Prozess zum Management von Informationssicherheitsvorfällen dokumentiert werden, unter Berücksichtigung aller (gesetzlicher) bzw. internen Meldepflichten und Einbeziehung aller für die Beseitigung des Vorfalls interner bzw. externer Stellen.

Es sollte eine klare Verantwortlichkeit für das Incident Management auf Seiten des Cloud-Anbieters festgelegt werden.

Relevante Informationen über Sicherheitsvorfälle aus Cloud-Diensten müssen in eine zentrale Überwachung integriert werden. Die Überwachung kann hierbei vom Cloud-Anbieter oder von der FMG betrieben werden. Sollte die Überwachung eines Cloud-Anbieters genutzt werden, muss festgelegt werden, wie die FMG informiert und eingebunden wird.

16.1.2 Melden von Informationssicherheitsereignissen

Maßnahme: Informationssicherheitsereignisse sollten so schnell wie möglich über geeignete Kanäle zu deren Handhabung gemeldet werden.

Jeder sicherheitsrelevante Vorfall muss dokumentiert und dem zuständigen Ansprechpartner gemeldet werden. Die Dokumentation muss mindestens die folgenden Punkte beinhalten:
a) Beschreibung des Vorfalls
b) Auswirkungen des Vorfalls
c) Reaktive Maßnahmen zur Schadensbeseitigung
d) Vorschlag für zukünftige proaktive Maßnahmen
Allen Angestellten, Auftragnehmern und Drittbenutzern muss die Verpflichtung zur Meldung sicherheitsrelevanter Vorfälle bekannt sein. Dies beinhaltet auch die Kenntnis des Meldeverfahrens und des betreffenden Ansprechpartners.

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.

Der Cloud-Anbieter muss mit der FMG abstimmen, über welche technischen Wege über sicherheitsrelevante Ereignisse informiert wird.

Hierzu müssen auch die folgenden Punkte umgesetzt werden:
- Benennung einer Kontaktstelle für die Meldung von Incidents und zum Erhalt von Informationen über Incidents (Ansprechpartner, E-Mail, optimalerweise Telefonnummer sowie Kontaktzeiten) beim Cloud-Anbieter und bei der FMG
- Definition der Schnittstellen für die Behandlung von Incidents mit Einfluss auf die FMG und den Cloud-Anbieter
- Definition von gegenseitigen Informationspflichten und -Fristen zu aktuellen / aufgetretenen Incidents.
- Die FMG muss über alle Incidents informiert werden, die potenziellen Bezug auf Daten oder Systeme der FMG haben

16.1.3 Meldung von Schwächen in der Informationssicherheit

Maßnahme: Beschäftigte und Auftragnehmer, welche die Informationssysteme und -dienste der Organisation nutzen, sollten dazu angehalten werden, jegliche beobachteten oder vermuteten Schwächen in Systemen oder Diensten festzuhalten und zu melden.

Jede Sicherheitsschwachstelle muss dem zuständigen Ansprechpartner gemeldet werden, um sicherheitsrelevante Vorfälle zu vermeiden.

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.

16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse

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

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Maßnahme: Auf Informationssicherheitsvorfälle sollte entsprechend den dokumentierten Verfahren reagiert werden.

BSIG-71: Die Bewertung bzw. Behandlung von Informationssicherheitsvorfällen, darf nur durch autorisiertes und qualifiziertes Personal durchgeführt werden.

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Verantwortliche Rollen: Auftraggeber/Projektmanager extern, IS-Beauftragter/Bereichs-IS-Beauftragter

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

Die Informationen, die durch die Auswertung von Informationssicherheitsvorfällen erhalten wurden, sollten dazu dienen, um sich wiederholende Vorfälle oder Vorfälle mit großer Auswirkung zu identifizieren.
Die Auswertung von Informationssicherheitsvorfällen kann den Bedarf für verbesserte oder zusätzliche Maßnahmen aufzeigen, um die Häufigkeit, den Schaden und die Kosten bei zukünftigen Vorfällen zu begrenzen, oder um im Überprüfungsprozess für die Sicherheitsleitlinie berücksichtigt zu werden (siehe 5.1.2).

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.

16.1.7 Sammeln von Beweismaterial

Maßnahme: Die Organisation sollte Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Information, die als Beweismaterial dienen kann, festlegen und anwenden.

Für die Sammlung gerichtlich verwertbarer Beweise müssen interne Verfahren entwickelt und befolgt werden. Es müssen forensische Verfahren für die gängigen Systeme (IT, OT, IoT, ICS, ...) erstellt werden. Diese müssen u.a. die nachfolgenden Aspekte berücksichtigen:

a) Bei Papierdokumenten: Das Original wird sicher verwahrt, und es wird aufgezeichnet, wer es gefunden hat, wo es gefunden wurde, wann es gefunden wurde und wer Zeuge bei der Entdeckung war; Untersuchungen müssen sicherstellen, dass die Originale nicht verfälscht wurden;
b) Bei Informationen auf Computermedien: Zur Sicherstellung, dass Informationen verfügbar sind, müssen Spiegelungen oder Kopien aller mobilen Datenträger, Informationen auf Festplatten oder im Speicher erstellt werden; das Protokoll aller Tätigkeiten während des Kopierprozesses muss aufbewahrt und der

Prozess von einem Zeugen beobachtet werden; das Original des Datenträgers und das Protokoll (falls dies nicht möglich ist, dann zumindest eine Spiegelung oder Kopie) müssen sicher verwahrt werden und unangetastet bleiben.
Jegliche forensische Arbeit darf nur an Kopien des Beweismaterials durchgeführt werden.

Luftverkehrsspezifische Umsetzungsvorgaben

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

Der Cloud-Anbieter muss das Sammeln von digitalen Beweismitteln ermöglichen und aktiv unterstützen.

17 Informationssicherheitsaspekte beim Business Continuity Management

17.1 Aufrechterhalten der Informationssicherheit

Ziel: Die Aufrechterhaltung der Informationssicherheit sollte in das Business Continuity Managementsystem der Organisation eingebettet sein.

17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit

Maßnahme: Die Organisation sollte ihre Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements bei widrigen Situationen bestimmen, z. B. Krisen oder Katastrophen.

Risikoeinschätzungen zur Sicherstellung des Geschäftsbetriebs müssen unter voller Einbeziehung der Eigentümer von Geschäftsressourcen und Prozessen durchgeführt werden.
Die Einschätzung muss die Risiken identifizieren, quantifizieren und nach Kriterien und Zielen priorisieren, die für die Organisation wichtig sind.
Abhängig von den Ergebnissen der Risikoeinschätzung muss eine Strategie zur Sicherstellung des Geschäftsbetriebs entwickelt werden, um den Gesamtansatz der Sicherstellung des Geschäftsbetriebs festzulegen.
Diese Strategie ist vom Management freizugeben, und es ist daraus resultierend ein Plan zur Umsetzung dieser Strategie zu erstellen.

BSIG-17: Es muss ein Verantwortlicher für BCM festgelegt werden.

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;
- Festlegung von Kritikalitätskategorien und Schadensszenarien;
- Festlegung der zu betrachtenden Bewertungszeiträume;
- besondere Termine und Ereignisse;
- Kritikalitätsanalyse;
- Priorisierung der einzelnen Prozesse;
- Übersicht über Ressourcen für Normal- und Notbetrieb;

- Kritikalität und Wiederanlaufzeiten der Ressourcen;
- Berichterstattung.

Werden im laufenden Prozess Werte ausgetauscht, so dass Änderungen in der Geschäftsauswirkungsanalyse nicht ausgeschlossen werden können, sollte die Geschäftsauswirkungsanalyse wiederholt werden. Die am Geschäftsprozess beteiligten Partner müssen umgehend darüber informiert werden.

Im Rahmen der Geschäftsauswirkungsanalyse muss eine Planung für einen Betrieb der Anwendung ohne Cloud erstellt werden. Dieser muss im Rahmen einer Exit Strategie (z.B. falls der Cloud-Dienst eingestellt wird) erfolgen.

17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit

Maßnahme: Die Organisation sollte Prozesse, Verfahren und Maßnahmen festlegen, dokumentieren, umsetzen und aufrechterhalten, um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können.

BSIG-18: Für kritische IT-Systeme bzw. –Szenarien müssen Notfallpläne, sowie zusätzlich erforderliche Dokumente, für die Bewältigung eines IT-Notfalls erstellt werden. Diese Pläne bzw. Dokumente müssen folgendes beinhalten:

a) Definition von Verantwortlichen und für den IT-Notfall einzubeziehenden Ansprechpartner.
b) Definition von Abhängigkeiten zu anderen IT-Systeme, bzw. Festlegung der erforderlichen Ressourcen zur Bewältigung des IT-Notfalls.

17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit

Maßnahme: Die Organisation sollte in regelmäßigen Abständen die festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit überprüfen, um sicherzustellen, dass diese gültig und in widrigen Situationen wirksam sind.

BSIG-19: Notfallpläne müssen regelmäßig (= mindestens jährlich) durch die beteiligten Organisationen überprüft, und getestet. Die daraus gewonnenen Ergebnisse müssen Input für die Verbesserung und Aktualisierung der Notfallpläne sein. Die durchgeführten Tests müssen dokumentiert werden. Um das Funktionieren der Notfallpläne sicherzustellen, müssen die beteiligten Organisationen folgendes durchführen:

a) Test und Abnahme der Notfallpläne vor Inbetriebnahme des Systems
b) Test und Abnahme der Notfallpläne bei kritischen System- und Prozessänderungen
c) Regelmäßiger (= mind. jährlicher) Test aller Notfallpläne

Art und Umfang der Tests müssen sich an der Kritikalität des Geschäftsprozesses orientieren.
Die Verantwortung für regelmäßige Überprüfungen der Pläne zur Sicherstellung des Geschäftsbetriebs muss geregelt sein.
Verlauf und Ergebnisse der Tests müssen aufgezeichnet werden, und bei Bedarf sind Maßnahmen zu ergreifen und die Pläne zu optimieren.

Luftverkehrsspezifische Umsetzungsvorgaben

Das Rahmenwerk für Kontinuitätspläne sollte einen Terminplan für die Überprüfung und Aktualisierung der Kontinuitätspläne enthalten.
Kontinuitätspläne sollten regelmäßig durch die beteiligten Organisationen gemeinsam geprüft werden. Die daraus gewonnenen Informationen sollten als Eingabe für die Verbesserung und Aktualisierung der Kontinuitätspläne dienen. Die Prüfungen sollten dokumentiert werden. Um das ordnungsgemäße Funktionieren der

Kontinuitäts-Kontingenzpläne sicherzustellen, sollten die beteiligten Organisationen folgende Maßnahmen durchführen:
Die Prüfung und Abnahme der Pläne sollte vor

- Inbetriebnahme des Systems/des Geschäftsprozesses,
- kritischen System- und Prozessänderungen erfolgen.
- Der Anwendungsbereich der Prüfungen sollte sich an der Kritikalität des Geschäftsprozesses orientieren.

17.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs

Maßnahme: Ein Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs muss festgelegt werden, um so sicherzustellen, dass alle Pläne widerspruchsfrei sind, um Informationssicherheitsanforderungen einheitlich zu behandeln, und um Prioritäten für Tests und Instandhaltung zu identifizieren

Anforderung

- Der Prozess für ein Business Continuity Management muss mindestens die nachfolgenden Punkte enthalten:

a) Identifikation aller organisationseigenen Werte, die zu kritischen Geschäftsprozessen gehören
b) Verstehen der Auswirkungen, die Informationssicherheitsvorfälle wahrscheinlich auf das Geschäft haben werden sowie Festlegung der Organisationsziele für Anwendungen und Systeme
c) Identifikation von zusätzlichen vorbeugenden und schadensmildernden Maßnahmen und Überlegungen zu deren Umsetzung
d) Formulierung und Dokumentation von Plänen zur Sicherstellung des Geschäftsbetriebs, die die Informationssicherheitsanforderungen in Übereinstimmung mit der vereinbarten Strategie zur Sicherstellung des Geschäftsbetriebs behandeln
e) regelmäßige Tests und Aktualisierungen der etablierten Pläne und Prozesse

- Auf Basis der Risikoeinschätzung müssen die beteiligten Bereiche einen Notfallplan erstellen. Dieser muss zumindest beinhalten:

a) Verantwortlichkeiten
b) Notfall-Situationen
c) Ausweichmaßnahmen, alternative Betriebsverfahren
d) Detaillierte Beschreibung der relevanten Notfallmaßnahmen
e) Regelungen zu Prüfungen und Aktualisierungen der Notfallpläne

- Der Rahmen für die Pläne zur Sicherstellung des Geschäftsbetriebs muss die identifizierten Informationssicherheitsanforderungen behandeln und die folgenden Elemente berücksichtigen:

a) die Bedingungen zum Inkrafttreten der Pläne, die den zu befolgenden Prozess beschreiben, bevor jeder Plan in Kraft tritt;
b) Notfall-Verfahren, die die Aktionen beschreiben, die nach einem Vorfall zu ergreifen sind, der Geschäftsabläufe gefährdet;
c) Ausweichmaßnahmen, die die Aktionen beschreiben, die zu ergreifen sind, um wichtige Geschäftsaktivitäten oder unterstützende Dienste vorübergehend zu alternativen Standorten umzusiedeln, und um Geschäftsprozesse innerhalb des geforderten Zeitraums wieder zum Laufen zu bringen;
d) ein Wartungsplan, welcher spezifiziert, wie und wann der Plan getestet wird, und der Prozess zur Pflege des Plans;
e) Maßnahmen zur Sensibilisierung, Ausbildung und Schulung, die entwickelt wurden, um Verständnis für die Prozesse zur Sicherstellung des Geschäftsbetriebs zu schaffen, und um sicherzustellen, dass die Prozesse weiterhin wirksam bleiben;
f) die Verantwortung einzelner Personen, mit einer Beschreibung, wer für die Ausführung welcher Komponente des Plans verantwortlich ist. Vertreter müssen je nach Bedarf benannt sein.

Luftverkehrsspezifische Umsetzungsvorgaben

Die beteiligten Organisationen sollten einen organisationsübergreifenden Rahmen für den Plan zur Sicherstellung des Geschäftsbetriebs erstellen, der auf der Geschäftsauswirkungsanalyse beruht. Folgendes sollte darin mindestens enthalten sein:

- Personen in verantwortlichen Positionen bezüglich der gemeinschaftlichen Entscheidungsfindung;
- Notfallszenarien, die mehrere Organisationen betreffen,
- alternative Maßnahmen;
- alternative Betriebsverfahren;
- Aufbau der Kontinuitätspläne.

Aufgrund der geforderten hohen Verfügbarkeit von Geschäftsprozessen in der Luftfahrt sollte die Organisation in ihren Betriebsprozessen die Umstände dokumentieren, unter denen Kontinuitäts- oder Krisenpläne aktiviert werden.

Kündigungsfristen für Cloud-Dienste müssen dem Einsatzszenario entsprechend angemessen sein. Soweit rechtlich möglich, sollten kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der FMG vermieden werden.

17.2 Redundanzen

Ziel: Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.

17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

Maßnahme: Informationsverarbeitende Einrichtungen sollten mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.

18 Compliance

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

Ziel: Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und gegen jegliche Sicherheitsanforderungen sind vermieden.

18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

Maßnahme: Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen der Organisation zur Einhaltung dieser Anforderungen sollten für jedes Informationssystem und die Organisation ausdrücklich bestimmt, dokumentiert und auf dem neuesten Stand gehalten werden.

Luftverkehrsspezifische Umsetzungsvorgaben

Verpflichtungen zum Schutz kritischer Infrastrukturen auf nationaler und Europäischer Ebene könnten betrachtet werden.

Vereinbarungen zu Cloud-Diensten dürfen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren geschlossen werden.

Die Verarbeitung von Daten in Cloud-Diensten darf ausschließlich auf IT-Systemen in Europa stattfinden.

18.1.2 Geistige Eigentumsrechte

Maßnahme: Es sollten angemessene Verfahren umgesetzt werden, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und die Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Die Mitarbeiter sind in Bezug auf die Leitlinie zu sensibilisieren.
Die Beschaffung von Software darf nur über seriöse Anbieter erfolgen, um sicherzustellen, dass das Urheberrecht nicht verletzt wird.
Es ist sicherzustellen, dass zu jeder Zeit geeignete Nachweise für den Erwerb von Nutzungsrechten/Lizenzen erbracht werden können.
Es sind Maßnahmen zu etablieren, die garantieren, dass die Nutzungsrechte des Herstellers eingehalten werden.
Es sind regelmäßige Überprüfungen des eingesetzten Softwarebestandes vorzunehmen, um zu gewährleisten, dass nur genehmigte Software und lizenzierte Produkte installiert sind.

Es muss im Vorfeld des Einsatzes eines Cloud-Dienstes geprüft werden, ob lizensierte Software in Cloud-Umgebungen eingesetzt werden kann und ob dies im Rahmen der erworbenen Lizenz erlaubt ist. Hierbei müssen insbesondere alle Produkte geprüft werden, welche auf Basis von CPUs oder Speicher abgerechnet werden.

18.1.3 Schutz von Aufzeichnungen

Maßnahme: Aufzeichnungen sollten gemäß der gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.

Es sind Regelungen für die Aufbewahrung, Speicherung, Handhabung und Entsorgung von Aufzeichnungen und Informationen zu erstellen.
Ein Aufbewahrungsverzeichnis muss erstellt werden, das die Aufzeichnungen und die erforderlichen Aufbewahrungsfristen festlegt.
Es sind angemessene Maßnahmen umzusetzen, die Aufzeichnungen und Informationen vor Verlust, Zerstörung und Fälschung schützen. Dabei ist sicherstellen, dass verschlüsselte Informationen innerhalb des erforderlichen Zeitraums wieder entschlüsselt werden können.

18.1.4 Privatsphäre und Schutz von personenbezogener Information

Maßnahme: Die Privatsphäre und der Schutz von personenbezogener Information sollten, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sichergestellt werden.

Es ist mindestens eine Datenschutz- und Vertraulichkeitsleitlinie zu entwickeln und umzusetzen. Diese Leitlinie ist allen Personen bekannt zu machen, die an der Verarbeitung personenbezogener Daten beteiligt sind.
Die Verantwortung für den Umgang mit personenbezogenen Daten ist in Übereinstimmung mit den geltenden Gesetzen und Vorschriften zu definieren.

Bei Einsatz eines Cloud-Dienstes muss die Rückgabe der Daten vertraglich geregelt werden (Format, Datenträger, Protokolle, usw.).
Die Löschfristen der Kundendaten nach Kündigung sollten vertraglich vereinbart werden.
Die Löschung der Kundendaten (inkl. Datensicherung) sollten durch den Cloud-Anbieter schriftlich an die FMG bestätigt werden. Die Bestätigung muss auch Daten bei Unterauftragsnehmern des Cloud-Anbieters umfassen.

Sofern im Cloud-Dienst personenbezogene Daten im Auftrag verarbeitet werden, muss ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Der Auftraggeber bzw. Kostenstellenverantwortliche muss mindestens jährlich die „Einhaltung der datenschutzrechtlichen Vorschriften" vom Cloud-Anbieter bestätigen lassen.

Es dürfen nur Cloud-Anbieter beauftragt werden, welche hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen etabliert sind, dass die Verarbeitung im Einklang mit den Datenschutzvorschriften erfolgt.

18.1.5 Regelungen bezüglich kryptographischer Maßnahmen

Maßnahme: Kryptographische Maßnahmen sollten unter Einhaltung aller relevanten Vereinbarungen, Gesetze und Vorschriften angewandt werden.

Es sind Verfahren/Regelungen für die Nutzung von kryptografischen Maßnahmen zu etablieren, die mindestens die nachstehenden Aspekte berücksichtigen. Bei der Erstellung ist juristischer Rat einzuholen, um sicherzustellen, dass die Einhaltung der entsprechenden Gesetze gewährleistet ist.

a) Einschränkungen bezüglich des Imports und/oder Exports von Hard- und Software, die kryptographische Funktionen ausführen
b) Einschränkungen bezüglich des Imports und/oder Exports von Hard- und Software, die so gestaltet ist, dass kryptographische Funktionen hinzugefügt werden können
c) Einschränkungen bezüglich des Gebrauchs von Verschlüsselungsverfahren
d) Einschränkungen bei der Einführung verschlüsselter Systeme in bestimmte Länder

18.2 Überprüfungen der Informationssicherheit

Ziel: Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und wird entsprechend angewendet.

18.3 Unabhängige Überprüfung der Informationssicherheit

Maßnahme: Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung (d. h. Maßnahmenziele, Maßnahmen, Richtlinien, Prozesse und Verfahren zur Informationssicherheit) sollten auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.

a) Regelmäßige Überprüfung (= mindestens jährlich) der Einhaltung der aller anwendbaren externen und internen Vorgaben (u.a. definiert in Richtlinien und Prozessbeschreibungen) zur Informationssicherheit.
b) Untersuchung von Möglichkeiten zur Verbesserung und Untersuchungen des Bedarfs für Änderungen am generellen Ansatz für Sicherheit, einschließlich der Leitlinie und der Maßnahmenziele beinhalten.
c) Priorisierung der identifizierten Verbesserungsmöglichkeiten.
d) Die Abarbeitung der identifizierten Maßnahmen muss regelmäßig überprüft werden.
e) Die Ergebnisse der unabhängigen Überprüfung müssen aufgezeichnet Aufzeichnung der Ergebnisse der unabhängigen Überprüfung inkl. Berichterstattung an das Management.

18.3.1 Einhaltung von Sicherheitsrichtlinien und -standards

Maßnahme: Leitende Angestellte sollten regelmäßig die Einhaltung der jeweils anzuwendenden Sicherheitsrichtlinien, Standards und jeglicher sonstigen Sicherheitsanforderungen bei der Informationsverarbeitung und den Verfahren in ihrem Verantwortungsbereich überprüfen.

Manager müssen regelmäßig die Einhaltung der in ihrem Verantwortungsbereich stattfindenden Informationsverarbeitung mit anwendbaren Sicherheitsleitlinien, -standards und allen anderen Sicherheitsanforderungen überprüfen.
Sofern im Rahmen der Überprüfungen Abweichungen festgestellt werden, muss der Manager sicherstellen, dass

a) der Bedarf für Maßnahmen bewertet wird, um sicherzustellen, dass die Abweichung nicht wieder auftritt
b) angemessene Korrekturmaßnahmen festgelegt und umsetzt werden
c) die ergriffenen Korrekturmaßnahmen überprüft werden

BSIG-67: Ausnahmen bzw. Abweichungen von den Regeln in den Informationssicherheitsrichtlinien müssen dokumentiert und regelmäßig (d.h. zumindest jährlich) überprüft werden.

18.3.2 Überprüfung der Einhaltung von technischen Vorgaben

Maßnahme: Informationssysteme sollten regelmäßig auf Einhaltung der Informationssicherheitsrichtlinien und -standards der Organisation überprüft werden.

Regelmäßige Überprüfung (= mindestens jährlich) der Einhaltung der technischen Vorgaben zur Informationssicherheit in den betriebenen IT-Systemen.
Prüfungen der Einhaltung technischer Standards müssen entweder manuell (falls nötig mit Unterstützung geeigneter Software-Tools) durch einen erfahrenen Systemingenieur und/oder mit Hilfe von automatisierten Tools durchgeführt werden, die einen technischen Bericht erzeugen, der anschließend durch einen technischen Spezialisten interpretiert wird.
Falls Penetrationstests oder Schwachstellenanalysen durchgeführt werden, so müssen diese mit Vorsicht geschehen, da solche Aktivitäten die Sicherheit des Systems gefährden könnten. Solche Tests müssen geplant und dokumentiert werden und wiederholbar sein. Alle Prüfungen der Einhaltung technischer Standards müssen nur durch kompetente, berechtigte Mitarbeiter oder unter der Aufsicht solcher Experten erfolgen.
Qualifiziertes Personal (z. B. Interne Revision) oder sachverständige Dritte überprüfen mindestens jährlich die Compliance der IT-Systeme mit den entsprechenden internen Richtlinien und Standards sowie der für die kritischen Dienstleistungen relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen.

Anhang 1: Beispieltabelle zur Zuordnung von Mindestverantwortlichkeiten der Informationssicherheit

Wert	Verantwortliche	Prozesse
Zugangsweg (z.B. WLAN, UMTS, Ethernet)		
Zone (z.B. internes Netz, eigenes VPN, externes Netz)		
Informationsverantwortlicher (Festlegung: Vertraulichkeit, Verfügbarkeit, Berechtigungen)		
Applikation		
Genutzte Applikationen (z.B. Apache, Tomcat)		
Runtime (z.B. Applikationsserver, Netframework, Java)		
Datenbank		
Middleware		
OS		
Virtueller Server		
Virtualisierungslösung		
Physikalische Server / Device		
Firewall		
Netzwerk		
Physikalischer Zugang (z.B. zum jeweiligen Server, Inforaum, Büro, RZ)		

20 Anhang 2: Zuordnung Controls zu Level of Trust, Vertraulichkeit und Verfügbarkeit

Die folgende Tabelle gibt einen Überblick über die zu erfüllenden Controls beim jeweiligen Level of Trust (LT). Zusätzlich stellt sie den jeweiligen Schutzbedarf aus Vertraulichkeits- bzw. Verfügbarkeits-Gesichtspunkt dar, ab dem das betreffende Controls ebenfalls umzusetzen ist.

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
5 Sicherheitsleitlinie					
5.1 Informationssicherheitsleitlinie					
5.1.1 Vorgaben der Leitung für Informationssicherheit	X	X	X	dienstlich	mittel
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	X	X	X	dienstlich	mittel

CoPiP Controls aus ISO27001:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
5.2 Führung					
5.2.1 Führung und Verpflichtung (Referenz Kapitel 5.1)	X	X	X	dienstlich	mittel
5.2.2 Politik (Referenz Kapitel 5.2)	X	X	X	dienstlich	mittel
5.2.3 Managementbewertung (Referenz Kapitel 9.3)	X	X		vertraulich	hoch
5.2.4 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation (Referenz Kapitel 5.3)	X	X	X	dienstlich	mittel
5.2.5 Überwachung, Messung, Analyse & Bewertung (Referenz Kapitel 9.1)	X	X		vertraulich	hoch
5.2.6 Dokumentierte Information (Referenz Kapitel 7.5)	X	X		vertraulich	hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
6 Organisation der Informationssicherheit					
6.1 Interne Organisation					
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten	X	X	X	dienstlich	mittel
6.1.2 Aufgabentrennung	X			streng vertraulich	sehr hoch
6.1.3 Kontakt mit Behörden	X			streng vertraulich	sehr hoch
6.1.4 Kontakt mit speziellen Interessensgruppen	X			streng vertraulich	sehr hoch
6.1.5 Informationssicherheit im Projektmanagement	X			streng vertraulich	sehr hoch
6.2 Mobilgeräte und Telearbeit					
6.2.1 Richtlinie zu Mobilgeräten	X	X		vertraulich	hoch
6.2.2 Telearbeit	X	X		vertraulich	hoch
7 Personalsicherheit					
7.1 Vor der Beschäftigung					
7.1.1 Sicherheitsüberprüfung	X	X		vertraulich	hoch
7.1.2 Beschäftigungs- und Vertragsbedingungen	X			streng vertraulich	sehr hoch
7.2 Während der Anstellung					
7.2.1 Verantwortlichkeiten der Leitung	X	X		vertraulich	hoch
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung	X	X	X	dienstlich	mittel
7.2.3 Maßregelungsprozess	X			streng vertraulich	sehr hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
7.3 Beendigung und Änderung der Beschäftigung					
7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	X			streng vertraulich	sehr hoch
8 Verwaltung der Werte					
8.1 Verantwortlichkeit für Werte					
8.1.1 Inventarisierung der Werte	X	X	X	dienstlich	mittel
8.1.2 Zuständigkeit für Werte	X	X		vertraulich	hoch
8.1.3 Zulässiger Gebrauch von Werten	X			streng vertraulich	sehr hoch
8.1.4 Rückgabe von Werten	X	X		vertraulich	hoch
8.2 Informationsklassifizierung					
8.2.1 Klassifizierung von Information	X	X	X	dienstlich	mittel
8.2.2 Kennzeichnung von Information	X	X		vertraulich	hoch
8.2.3 Handhabung von Werten	X	X		vertraulich	hoch
8.3 Handhabung von Datenträgern					
8.3.1 Handhabung von Wechseldatenträgern	X			streng vertraulich	sehr hoch
8.3.2 Entsorgung von Datenträgern	X			streng vertraulich	sehr hoch
8.3.3 Transport von Datenträgern					
9 Zugangssteuerung					
9.1 Geschäftsanforderungen an die Zugangssteuerung					
9.1.1 Zugangssteuerungsrichtlinie	X	X	X	dienstlich	mittel

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
9.1.2 Zugang zu Netzwerken und Netzwerkdiensten	X			streng vertraulich	sehr hoch
9.2 Benutzerzugangsverwaltung					
9.2.1 Registrierung und Deregistrierung von Benutzern	X	X	X	dienstlich	mittel
9.2.2 Zuteilung von Benutzerzugängen	X	X		vertraulich	hoch
9.2.3 Verwaltung privilegierter Zugangsrechte	X	X	X	dienstlich	mittel
9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern	X	X		vertraulich	hoch
9.2.5 Überprüfung von Benutzerzugangsrechten	X	X		vertraulich	hoch
9.2.6 Entzug oder Anpassung von Zugangsrechten	X	X	X	dienstlich	mittel
9.2.7 Digitales Identitätsmanagement (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
9.2.8 Organisationsübergreifende eindeutige Darstellung von Entitäten (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
9.3 Benutzerverantwortlichkeiten					
9.3.1 Gebrauch geheimer Authentisierungsinformation	X	X	X	dienstlich	mittel
9.4 Zugangssteuerung für Systeme und Anwendungen					
9.4.1 Informationszugangsbeschränkung	X	X	X	dienstlich	mittel
9.4.2 Sichere Anmeldeverfahren	X	X	X	dienstlich	mittel
9.4.3 System zur Verwaltung von Kennwörtern	X	X		vertraulich	hoch
9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten					

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
9.4.5 Zugangssteuerung für Quellcode von Programmen	X			streng vertraulich	sehr hoch
9.4.6 Web-Application Firewalls (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
10 Kryptographie					
10.1 Kryptographische Maßnahmen					
10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen	X			streng vertraulich	sehr hoch
10.1.2 Schlüsselverwaltung	X			streng vertraulich	sehr hoch
11 Physische und umgebungsbezogene Sicherheit					
11.1 Sicherheitsbereiche					
11.1.1 Physische Sicherheitsperimeter	X	X	X	dienstlich	mittel
11.1.2 Physische Zutrittssteuerung	X	X	X	dienstlich	mittel
11.1.3 Sichern von Büros, Räumen und Einrichtungen	X			streng vertraulich	sehr hoch
11.1.4 Schutz vor externen und umweltbedingten Bedrohungen	X			streng vertraulich	sehr hoch
11.1.5 Arbeiten in Sicherheitsbereichen					
11.1.6 Anlieferungs- und Ladebereiche	X			streng vertraulich	sehr hoch
11.2 Geräte und Betriebsmittel					
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln	X	X		vertraulich	hoch
11.2.2 Versorgungseinrichtungen	X	X	X	dienstlich	mittel

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
11.2.3 Sicherheit der Verkabelung	X			streng vertraulich	sehr hoch
11.2.4 Instandhaltung von Geräten und Betriebsmitteln	X			streng vertraulich	sehr hoch
11.2.5 Entfernen von Werten	X			streng vertraulich	sehr hoch
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	X			streng vertraulich	sehr hoch
11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	X			streng vertraulich	sehr hoch
11.2.8 Unbeaufsichtigte Benutzergeräte	X	X	X	dienstlich	mittel
11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	X			streng vertraulich	sehr hoch
12 Betriebssicherheit					
12.1 Betriebsabläufe und -verantwortlichkeiten					
12.1.1 Dokumentierte Betriebsabläufe	X	X		vertraulich	hoch
12.1.2 Änderungssteuerung	X	X		vertraulich	hoch
12.1.3 Kapazitätssteuerung					
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen	X			streng vertraulich	sehr hoch
12.2 Schutz vor Schadsoftware					
12.2.1 Maßnahmen gegen Schadsoftware	X	X	X	dienstlich	mittel
12.3 Datensicherung					
12.3.1 Sicherung von Information	X	X		vertraulich	hoch
12.4 Protokollierung und Überwachung					

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
12.4.1 Ereignisprotokollierung	X			streng vertraulich	sehr hoch
12.4.2 Schutz der Protokollinformation	X			streng vertraulich	sehr hoch
12.4.3 Administratoren- und Bedienerprotokolle	X	X		vertraulich	hoch
12.4.4 Uhrensynchronisation	X			streng vertraulich	sehr hoch
12.5 Steuerung von Software im Betrieb					
12.5.1 Installation von Software auf Systemen im Betrieb	X			streng vertraulich	sehr hoch
12.6 Handhabung technischer Schwachstellen					
12.6.1 Handhabung von technischen Schwachstellen	X	X	X	dienstlich	mittel
12.6.2 Einschränkungen von Softwareinstallation	X			streng vertraulich	sehr hoch
12.7 Audits von Informationssystemen					
12.7.1 Maßnahmen für Audits von Informationssystemen	X	X		vertraulich	hoch
12.7.2 Penetrationsprüfungen von Anwendungen (Zusätzliches CoPiP Control)	X	X	X	dienstlich	mittel
12.7.3 Penetrationsprüfungen von Infrastrukturen (Zusätzliches CoPiP Control)	X	X	X	dienstlich	mittel
13 Kommunikationssicherheit					
13.1 Netzwerksicherheitsmanagement					
13.1.1 Netzwerksteuerungsmaßnahmen	X	X	X	dienstlich	mittel
13.1.2 Sicherheit von Netzwerkdiensten	X	X		vertraulich	hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
13.1.3 Trennung in Netzwerken	X	X		vertraulich	hoch
13.2 Informationsübertragung					
13.2.1 Richtlinien und Verfahren für die Informationsübertragung	X	X		vertraulich	hoch
13.2.2 Vereinbarungen zur Informationsübertragung	X			streng vertraulich	sehr hoch
13.2.3 Elektronische Nachrichtenübermittlung					
13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen	X	X	X	dienstlich	mittel
14 Anschaffung, Entwicklung und Instandhaltung von Systemen					
14.1 Sicherheitsanforderungen an Informationssysteme					
14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen	X			streng vertraulich	sehr hoch
14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	X	X		vertraulich	hoch
14.1.3 Schutz der Transaktionen bei Anwendungsdiensten	X	X		vertraulich	hoch
14.1.4 Richtlinie für Webanwendungen/Web-Services	X			streng vertraulich	sehr hoch
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen					
14.2.1 Richtlinie für sichere Entwicklung	X			streng vertraulich	sehr hoch
14.2.2 Verfahren zur Verwaltung von Systemänderungen	X			streng vertraulich	sehr hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	X			streng vertraulich	sehr hoch
14.2.4 Beschränkung von Änderungen an Softwarepaketen					
14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	X			streng vertraulich	sehr hoch
14.2.6 Sichere Entwicklungsumgebung	X			streng vertraulich	sehr hoch
14.2.7 Ausgegliederte Entwicklung					
14.2.8 Testen der Systemsicherheit	X			streng vertraulich	sehr hoch
14.2.9 Systemabnahmetest	X			streng vertraulich	sehr hoch
14.2.10 Entwicklung von Anwendungen (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
14.2.11 Code-Reviews (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
14.3 Testdaten					
14.3.1 Schutz von Testdaten					
15 Lieferantenbeziehungen					
15.1 Informationssicherheit in Lieferantenbeziehungen					
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen	X	X		vertraulich	hoch
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen	X	X		vertraulich	hoch
15.1.3 Lieferkette für Informations- und Kommunikationstechnologie	X			streng vertraulich	sehr hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
15.2 Steuerung der Dienstleistungserbringung von Lieferanten					
15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen	X			streng vertraulich	sehr hoch
15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen	X			streng vertraulich	sehr hoch
16 Handhabung von Informationssicherheitsvorfällen					
16.1 Handhabung von Informationssicherheitsvorfällen und –verbesserungen					
16.1.1 Verantwortlichkeiten und Verfahren	X			streng vertraulich	sehr hoch
16.1.2 Melden von Informationssicherheitsereignissen	X	X		vertraulich	hoch
16.1.3 Meldung von Schwächen in der Informationssicherheit	X			streng vertraulich	sehr hoch
16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse	X	X		vertraulich	hoch
16.1.5 Reaktion auf Informationssicherheitsvorfälle	X	X		vertraulich	hoch
16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen	X			streng vertraulich	sehr hoch
16.1.7 Sammeln von Beweismaterial	X			streng vertraulich	sehr hoch
17 Informationssicherheitsaspekte beim Business Continuity Management					
17.1 Aufrechterhalten der Informationssicherheit					
17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit	X			streng vertraulich	sehr hoch

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit	X			streng vertraulich	sehr hoch
17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit					
17.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
17.2 Redundanzen					
17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen	X			streng vertraulich	sehr hoch
18 Compliance					
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen					
18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	X			streng vertraulich	sehr hoch
18.1.2 Geistige Eigentumsrechte					
18.1.3 Schutz von Aufzeichnungen					
18.1.4 Privatsphäre und Schutz von personenbezogener Information	X	X	X	dienstlich	mittel
18.1.5 Regelungen bezüglich kryptographischer Maßnahmen					
18.2 Überprüfungen der Informationssicherheit					
18.2.1 Unabhängige Überprüfung der Informationssicherheit	X			streng vertraulich	sehr hoch
18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards	X	X	X	dienstlich	mittel
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben	X	X	X	dienstlich	mittel

21 Inkrafttreten

Diese Richtlinie tritt am 19.07.2023 in Kraft.

22 Abkürzungsverzeichnis

siehe ISMS Glossar im Homebase.

23 Änderungshistorie

Org.-einheit	Bearbeiter	Datum (in Kraft treten)	Änderung	Versionsnummer
ITAI	Alexander Cmarits	01.07.2019	Erstfassung	001.001
ITAI	Alexander Cmarits	01.08.2020	Diverse kleinere Anpassungen	001.002
ITAI	Alexander Cmarits	19.07.2023	Aufnahme neuer Anforderungen (Konkretisierung aus dem BSIG §8a, DVO 2019/1583 2019 / 1583, Cyber Versicherung), redaktionelle Änderungen	002.001