Bundesministerium für Digitales und Verkehr

Grundsätze zur Anwendung der Cybersicherheitsmaßnahmen der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit

im Zuständigkeitsbereich des

Bundesministeriums für Digitales und Verkehr (§§ 9 und 9a LuftSiG)

Inkraftsetzung am:	31.05.2024
Vorlagepflicht (Punkt 1.6) ab:	01.01.2025

Inhaltsverzeichnis

Versionshistorie

Revision	Datum	Änderungen
1	31.05.2024	Initialversion
2	08.10.2024	Titel, 1.2, 1.4, 1.6, 2.2-2.6, 3.2, 3.3.2, 3.3.3, B.2.2, B.2.3

1 Grundsätzliches

1.1 Zielsetzung

Mit diesen Grundsätzen soll die Grundlage für eine einheitliche Auslegung der Durchführungsverordnung (EU) 2019/1583 der Europäischen Kommission vom 25. September 2019 zur Änderung der Verordnung (EU) 2015/1998 unter Einbeziehung des bereitgestellten unterstützenden Informationsmaterials geschaffen werden.

Die DVO (EU) 2019/1583 bezieht sich auf die Änderung 16 des Anhangs 17 (Security) des Abkommens über die internationale Zivilluftfahrt zur Festlegung gemeinsamer Standards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen.

Die Umsetzung der Cybersicherheitsmaßnahmen nach der DVO (EU) 2019/1583 gilt für sämtliche Luftfahrtunternehmen und Stellen, die die europäischen Grundstandards befolgen und Sicherheitsmaßnahmen gemäß Verordnung (EG) 300/2008 i. V. m. DVO (EU) 2015/1998 umsetzen.

1.2 Begriffsbestimmungen

1.2.1 Begriffsbestimmungen nach VO (EG) 300/2008 Art. 3

(1) Die **Luftsicherheit** ist die Kombination von

- Maßnahmen sowie
- personellen und
- materiellen Ressourcen,

die dazu dienen, die Zivilluftfahrt vor unrechtmäßigen Eingriffen zu schützen, die die Sicherheit der Zivilluftfahrt gefährden.[1]

(2) Ein **Betreiber** ist

- eine Person,
- eine Organisation oder
- ein Unternehmen,

die bzw. das Luftverkehrsaktivitäten durchführt oder anbietet[2].

(3) Ein **Luftfahrtunternehmen** ist ein Lufttransportunternehmen mit einer gültigen Betriebsgenehmigung oder einer gleichwertigen Genehmigung.[3]

[1] VO (EG) Nr. 300/2008 Artikel 3 Nr. 2
[2] VO (EG) Nr. 300/2008 Artikel 3 Nr. 3
[3] VO (EG) Nr. 300/2008 Artikel 3 Nr. 4

(4) Eine **Stelle** ist

- eine Person,
- eine Organisation oder
- ein Unternehmen,

die bzw. das kein Betreiber ist.[4]

1.2.2 Kritische informations- und kommunikationstechnische Systeme und Daten

(1) Ein System wird als **Informations- und Kommunikationssystem** verstanden, wenn es sich um

(a)

- ein Übertragungssystem,
- eine Vermittlungs- und Leitwegeinrichtung oder
- eine anderweitige Ressource, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen,

einschließlich

- Satellitennetze,
- feste (leitungs- und paketvermittelt, einschließlich Internet) und mobile Netze,
- Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden
- Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen;[5]

oder

(b)

- ein Gerät oder
- eine Gruppe miteinander verbundener oder zusammenhängender Geräte,

die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen[6]

handelt.[7]

[4] VO (EG) Nr. 300/2008 Artikel 3 Nr. 6
[5] Richtlinie (EU) 2018/1972 Artikel 2 Nummer 1
[6] Richtlinie (EU) 2022/2555
[7] AVSEC 10504 1.7.5 Background 7

(2) **Daten** sind relevant, wenn sie zum Zwecke

- des Betriebs,
- der Nutzung,
- des Schutzes oder
- der Pflege

von Informations- und Kommunikationssystemen

- gespeichert,
- verarbeitet,
- abgerufen,
- übertragen,
- gehalten,
- genutzt oder
- ausgetauscht

werden.[8]

(3) Systeme und Daten sind als **kritisch** zu bewerten, wenn der - auch nur teilweise - Verlust ihrer

- Vertraulichkeit,
- Integrität oder
- Verfügbarkeit

zur Ausführung eines widerrechtlichen, die Sicherheit der Zivilluftfahrt gefährdenden Eingriffs führen kann.
Diese Festlegung erfolgt ohne Berücksichtigung etwaiger vorhandener Gegenmaßnahmen.[9]

1.2.3 Weitere Begriffsbestimmungen

(1) Ein **Akteur** ist eine Sammelbezeichnung für

- Luftfahrtunternehmen,
- Betreiber und
- Stellen.[10]

(2) **Vertraulichkeit** ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[11]

[8] Richtlinie (EU) 2022/2555; AVSEC 10504 1.7.1 Background 2
[9] AVSEC 10504 1.7.1 Actions by the Air Carrier, Operator, Entity 1
[10] AVSEC 10504 Definition „*actor*"
[11] BSI Grundschutz-Kompendium Edition 2023 Glossar S. 8

(3) **Integrität** bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.[12]
(4) Die **Verfügbarkeit** von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.[13]
(5) Personen, die einen **unbeaufsichtigten und unbeschränkten Zugang** auf die für die Sicherheit in der Luftfahrt ermittelten kritischen informations- und kommunikationstechnischen Systeme und Daten haben, sind

- Mitarbeitende einer Institution,
- die im Rahmen der Erledigung ihrer Aufgaben auf der Basis der Rollenkonzepte Zugriffsrechte auf diese Systeme und Daten haben,
- dabei aber nicht über Administratorrechte zur Änderung der kritischen informations- und kommunikationstechnischen Systeme und Daten verfügen.

Dazu gehören auch die Mitarbeitenden eines IT-Dienstleistenden (externes Personal), die keine Administratorrechte haben, aber dennoch einen

- langfristigen
- regelmäßigen und
- unbeaufsichtigten

Zugang zu den kritischen informations- und kommunikationstechnischen Systemen und Daten haben.
(6) **Personen mit Administratorrechten**

- planen,
- installieren,
- betreiben,
- überwachen oder
- warten

die für die Sicherheit in der Luftfahrt kritischen informations- und kommunikationstechnischen Systeme und Daten und verfügen insbesondere und im Unterschied zur Gruppe der Personen gemäß Punkt 5 über Administrationsrechte zur Änderung dieser Systeme und Daten.
(7) Das **risk assessment**, als Bestandteil des Risikomanagements, umfasst die Unterprozesse

- risk identification (Erstellung einer Gefährdungsübersicht),
- risk analysis (Risikoeinschätzung) und
- risk evaluation (Risikobewertung)

In diesem Dokument wird der Begriff „*Risikobeurteilung*“ als Entsprechung für „*risk assessment*“ verwendet.

[12] BSI Grundschutz-Kompendium Edition 2023 Glossar S. 4
[13] BSI Grundschutz-Kompendium Edition 2023 Glossar S. 8

1.3 Zuständige Behörde

Im Luftsicherheitsgesetz vom 11. Januar 2005 in der Fassung des Ersten Gesetzes zur Änderung des Luftsicherheitsgesetzes vom 23. Februar 2017 (BGBl. I, S. 298) sind die für die Ausführung der Vorgaben der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72) („EG-Luftsicherheitsverordnung“) und der hierzu erlassenen Durchführungsbestimmungen zuständigen Luftsicherheitsbehörden festgelegt (§ 16 Abs. 2, 3 LuftSiG).

Zuständig für die Umsetzung der Cybersicherheitsmaßnahmen gemäß der durch die Verordnung (EU) 2019/1583 geänderten Fassung der Verordnung (EU) 2015/1998 in Bezug auf

- Luftfahrtunternehmen (§ 9 LuftSiG) und
- die sichere Lieferkette (§ 9a LuftSiG)

ist das dem Bundesministerium für Digitales und Verkehr nachgeordnete Luftfahrt-Bundesamt (LBA).[14]

Dies umfasst[15] insbesondere

- die Zulassung der Luftsicherheitsprogramme der Luftfahrtunternehmen und der Sicherheitsprogramme der Stellen und
- die Überwachung der Umsetzung der Cybersicherheitsmaßnahmen.[16]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) begleitet die Akteure fachlich bei der Umsetzung der in diesem Dokument dargelegten Cybersicherheitsmaßnahmen im Rahmen der durch BMDV und LBA gemachten Vorgaben.

Anfragen an das BSI können an das jeweils fachlich zuständige Referat unter LuSi@bsi.bund.de gerichtet werden.

[14] AVSEC 10504 1.7.4 Actions by the Appropriate Authority 1
[15] AVSEC 10504 1.7.4 Actions by the Appropriate Authority 2
[16] AVSEC 10504 1.7.4 Actions by the Appropriate Authority 3

1.4 Melde- und Informationswesen (DVO 2015/1998 Anhang Punkt 1.0.6)

Die Unterstützung bei der Durchführung einer wirksamen Risikobeurteilung ist von einem gegenseitigen Informationsaustausch[17] abhängig.

Die folgenden Verfahren stehen für diesen Austausch zur Verfügung:

(1) Informationen zu generellen Risiken einzelner Zielsysteme aber nicht zwangsläufig zu allen kritischen informations- und kommunikationstechnischen Systemen und Daten sind in den zutreffenden Bausteinen des BSI-Grundschutz auf der Webseite des BSI abrufbar.[18]

(2) Unter die Regulierung des Luftsicherheitsgesetzes fallende Unternehmen erhalten nach erfolgter Registrierung beim BSI von diesem

- werktags die Tageslageberichte mit allgemeinen Informationen zu Informationssicherheit
- anlassbezogen allgemeine und sektorspezifische Cyber-Sicherheitswarnungen (CSW).

Informationen dazu sind auf deren Webseite[19] abrufbar. [20]

(3) Meldungen erheblicher Störungen der Informationssicherheit sollten über das Melde- und Informationsportal[21] des BSI abgegeben werden. Diese Meldungen sind u. a. relevant um andere Akteure mittels Cyber-Sicherheitswarnungen über bestehende Risiken informieren zu können.

Eine erhebliche Störung der Informationssicherheit liegt insbesondere dann vor, wenn:

- eine Nicht-Reaktion negative Auswirkungen auf die Sicherheit der Zivilluftfahrt hat,
- zusätzliche Aufwände und Mittel zur Beseitigung der Störung eingesetzt werden müssen, die über die Aufwände und Mittel des Regelbetriebs oder bereits geplanter Arbeiten hinausgehen,
- die Beseitigung durch speziell vorgehaltene Incident-Responder oder Störfallteams durchgeführt werden muss,
- wichtige IT-Systeme oder Komponenten zur Vermeidung weiterer Auswirkungen abgeschaltet oder isoliert werden müssen,
- für den Bewältigungszeitraum Betriebsprozesse geändert werden müssen,
- sie einen hohen finanziellen Schaden verursacht oder
- der Verdacht besteht, dass das Unternehmen Ziel eines neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffs oder Angriffsversuchs ist.

(4) Aktuelle allgemeine Lagebilder der Bereiche Informationssicherheit und Cybercrime werden durch das BSI bzw. das Bundeskriminalamt bereitgestellt und sind über deren Webseiten[22] [23] abrufbar.[24]

[17] DVO (EU) 2015/1998 Anhang 1.0.6
[18] AVSEC 10504 1.0.6 Actions by the Appropriate Authority 2
[19] https://www.allianz-fuer-cybersicherheit.de
[20] AVSEC 10504 1.0.6 Actions by the Appropriate Authority 1
[21] https://mip2.bsi.bund.de/
[22] https://www.bka.de
[23] https://www.bsi.bund.de
[24] AVSEC 10504 1.7.3 Background 4

1.5 Alternative Rechtsvorschriften (DVO 2015/1998 Anhang Punkt 1.7.5)

Zur Vermeidung von Redundanzen oder Regelungslücken durch Überschneidungen von Cybersicherheitsanforderungen können durch nachweislich geltende und erfüllte alternative Rechtsvorschriften auch die Vorgaben des Anhangs 1.7 der DVO (EU) 2015/1998 als erfüllt gelten.

Einzelheiten hierzu sind künftig im, aktuell in Bearbeitung befindlichen, Anhang A aufgeführt.

1.6 Frist zur Vorlage

Die in diesem Dokument genannten Cybersicherheitsmaßnahmen sind ab dem 01.01.2025 zu berücksichtigen und in dem Sicherheitsprogramm zu beschreiben.

Ab dem vorgenannten Zeitpunkt müssen anlässlich

- einer erstmaligen Zulassung,
- einer wiederholenden Zulassung für Unternehmen nach §9a LuftSiG,
- einer Überprüfung der Zulassungsvoraussetzungen für Unternehmen nach §9 LuftSiG sowie
- einer Änderung der Zulassung

Sicherheitsprogramme vorgelegt werden, in denen die Maßnahmen zur Gewährleistung der Cybersicherheit beschrieben sind.

Für Sicherheitsprogramme, die einzig aufgrund der in diesem Dokument genannten Cybersicherheitsmaßnahmen angepasst werden, besteht zunächst keine Pflicht zur Vorlage.

Ausnahmeregelungen für Luftfahrtunternehmen mit Luftfahrzeugen bis 5,7 Tonnen MTOW („*Maximum Take Off Weight*“ oder Höchstabfluggewicht) und bekannte Lieferanten bleiben bestehen. Diese Akteure müssen weiterhin kein Luftsicherheitsprogramm einreichen, aber dennoch die erforderlichen Cybersicherheitsmaßnahmen gemäß den hier beschriebenen Vorgaben umsetzen.

2 Risikomanagement (DVO 2015/1998 Anhang Punkt 1.7.1 – 1.7.3)

Der Akteur implementiert einen Risikomanagementprozess unter Berücksichtigung der folgenden Unterabschnitte.

2.1 Geltungsbereich – Scope

Gegenstand des Risikomanagementprozesses sind informations- und kommunikationstechnische Systeme und Daten,[25] wenn diese

- aufgrund ihrer Bedeutung oder ihres Einflusses auf die Luftsicherheit als kritisch zu bewerten sind und
- in der Bundesrepublik Deutschland einer Interaktion zugeführt werden oder unter der deutschen Gerichtsbarkeit oder Zugehörigkeit stehen.[26]

2.2 Ermittlung kritischer informations- und kommunikationstechnischer Systeme und Daten

(1) Die Akteure ermitteln in eigener Verantwortung[27] ihre - für die Zivilluftfahrt genutzten - kritischen informations- und kommunikationstechnischen Systeme und Daten.[28] Dies erfolgt unabhängig des Umstandes, ob diese selbst betrieben werden oder der Betrieb durch Nachunternehmen, Dienstleister oder Drittanbieter[29] von den Akteuren beauftragt wurde.
Der Ermittlung werden die Begriffsbestimmungen aus Punkt 1.2 und ein prozessorientierter Ansatz, welcher in Anhang B Risikomanagement skizziert wird, zugrunde gelegt.

(2) Zu kritischen informations- und kommunikationstechnischen Systeme und Daten sind die folgenden Informationen zu erheben:

- Art des Einflusses auf die Luftsicherheit
- Anzahl der Nutzenden
- Verkaufender/Dienstleistender
- Softwareversion/Patch- oder Updatestand
- Art gespeicherter oder ausgetauschter Daten[30]

[25] DVO (EU) 2015/1998 Anhang 1.7.2/1.7.3
[26] AVSEC 10504 1.7.1 Background 2
[27] AVSEC 10504 1.7.2 Background 5
[28] DVO (EU) 2015/1998 Anhang 1.7.2
[29] AVSEC 10504 1.7.2 Background 14
[30] AVSEC 10504 1.7.3 Background 4 (g)

(3) Zur Bewertung des eigenen Gesamtrisikos und der entsprechenden Abhängigkeiten kann die Aufstellung der kritischen Nachunternehmen, Dienstleister und Drittanbieter sinnvoll sein. Hierbei sollten

- das kritische informations- und kommunikationstechnische System oder die Daten selbst,
- deren Systemgrenzen oder Einflussbereiche
- sowie die Ein- und Ausgangspunkte anderer - auch nicht kritischer - Komponenten innerhalb der Systemgrenzen oder des Einflussbereiches[31]

berücksichtigt werden.

Ob genutzte Produkte der Drittanbieter vom Grund auf sicher konzipiert wurden (security-by-design[32] -Ansatz), kann durch entsprechende

- Zertifikate
- Audits oder
- Testergebnisse[33]

überprüft werden.

(4) Wurden keine kritischen informations- und kommunikationstechnischen Systeme und Daten ermittelt, ist

- dieses Ergebnis,
- eine Beschreibung der angewandten Methodik[34] zur Ermittlung der kritischen informations- und kommunikationstechnischen Systeme und Daten und
- eine Beschreibung des im Unternehmen etablierten Risikomanagementsprozesses[35] für Cyberrisiken inklusive der einbezogenen Informationsquellen

im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument zu dokumentieren.

Eine weitere Bearbeitung des Kapitels 2 ist in diesem Fall nicht erforderlich.

(5) Eine nicht abschließende Übersicht beispielhafter kritischer informations- und kommunikationstechnischen Systeme und Daten und ein möglicher Weg der Ermittlung ebenjener befinden sich im Anhang B Risikomanagement dieses Dokuments.

[31] AVSEC 10504 1.7.2 Background 16
[32] AVSEC 10504 1.7.2 Background 17
[33] AVSEC 10504 1.7.3 Background 4 (i)
[34] AVSEC 10504 1.7.2 Background 7
[35] AVSEC 10504 1.0.6 Background 5

(6) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt.

1. Beschreibung der angewandten Methodik und einbezogenen Gruppen von Mitarbeitenden zur Ermittlung der kritischen informations- und kommunikationstechnischen Systeme und Daten.[36]
2. Auflistung der ermittelten kritischen informations- und kommunikationstechnischen Systeme und Daten. Dabei sind auch Systeme von Drittanbietern zu berücksichtigen und aufzuführen oder auf das entsprechende Sicherheitsprogramm des Drittanbieters zu verweisen.[37]

2.3 Risikobeurteilung - Risk assessment

(1) Die Akteure führen eine Risikobeurteilung hinsichtlich der ermittelten kritischen informations- und kommunikationstechnischen Systeme und Daten durch.[38]

(2) Eine umfängliche Risikobeurteilung besteht grundsätzlich aus den Schritten[39]

- Erstellung einer Gefährdungsübersicht - risk identification
- Risikoeinschätzung- risk analysis
- Risikobewertung - risk evaluation

(3) Die Erstellung einer Gefährdungsübersicht[40] und die Risikoeinschätzung erfolgt unter Berücksichtigung der im Rahmen des festgelegten Verfahrens des Informationswesen (siehe Abschnitt 1.4) erlangten zusätzlichen Informationen.[41]

(4) Die Risikobewertung ist mittels einer qualitativen Risikomatrix[42] durchzuführen.

Das Risiko-Level (level of risk) ist ab 60 % auf der Risikoskala als "inakzeptabel" zu bewerten.[43]

Eine beispielhafte Darstellung ist dem Anhang B Risikomanagement zu entnehmen.

(5) Die in Anhang B Risikomanagement hinterlegten Informationen können für eine Risikobeurteilung herangezogen werden.

(6) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt[44]:

- Beschreibung des Vorgehens zur Ermittlung von Cyberrisiken und der einbezogenen Informationsquellen, sowie des Ergebnisses der Risikoeinschätzung[45]
- Beschreibung der angewandten Risikobewertungsmethodik[46] und Darstellung der Ergebnisse der Risikobewertung.

[36] AVSEC 10504 1.7.2 Background 7
[37] AVSEC 10504 1.7.2 Background 14, AVSEC 10504 1.7.2 Actions by the Air Carrier, Operator, Entity 1
[38] AVSEC 10504 1.7.3 Background 1, AVSEC 10504 1.7.3 Background 2
[39] BSI-Standard 200-3 S. 51
[40] AVSEC 10504 1.7.3 Background 4 (e)(f)
[41] DVO (EU) 2015/1998 Anhang 1.0.6, AVSEC 10504 1.0.6 Background 1
[42] AVSEC 10504 11.1.2 Actions by the Air Carrier, Operator, Entity 2
[43] AVSEC 10504 1.7.2 Actions by the Appropriate Authority, AVSEC 10504 1.7.3 Actions by the Appropriate Authority 1
[44] AVSEC 10504 1.7.3 Background 1
[45] AVSEC 10504 1.0.6 Background 5
[46] AVSEC 10504 1.7.3 Actions by the Air Carrier, Operator, Entity 2

2.4 Risikobehandlung – Risk treatment

(1) Der Akteur ermittelt auf Grundlage der durchgeführten Risikobewertung[47] die inakzeptablen Risiken und setzt notwendige Maßnahmen zur Behandlung dieser um.

Dabei sind diese Maßnahmen

- in Zusammenhang mit den ermittelten Risiken zu bringen[48] und
- haben die Vertraulichkeit, Verfügbarkeit und Integrität im Fokus[49]

um das Restrisiko zu minimieren[50].

Zur Risikobehandlung von inakzeptablen Risiken sind ausschließlich Maßnahmen[51] der

- Risikovermeidung oder
- Risikoreduktion

gestattet.

Ein Risikotransfer oder eine Risikoübernahme sind nicht möglich

(2) Der Akteur implementiert und überwacht Maßnahmen zum Schutz der kritischen informations- und kommunikationstechnischen Systeme und Daten überdies auch bei

- Vor- und Nachunternehmen,
- Dienstleistern und
- Drittanbietern.[52]

(3) Die Maßnahmen sind so auszugestalten, dass nach deren Umsetzung das Risiko-Level (level of risk) die Risikoschwelle (risk threshold) zu „inakzeptabel" (definiert in Punkt 2.3 (4)) nicht überschreitet.[53]

Eine beispielhafte Darstellung ist dem Anhang B Risikomanagement zu entnehmen.

(4) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt:

Beschreibung der getroffenen Maßnahmen und deren Zusammenhang mit den Ergebnissen der durchgeführten Risikobewertung.

Im Detail werden hierzu die

- Maßnahmen,
- Instrumente,
- Hilfsmittel,
- Verfahren,
- Protokolle,
- Ressourcen und

[47] AVSEC 10504 1.7.2 Background 4
[48] AVSEC 10504 1.7.3 Actions by the Air Carrier, Operator, Entity 4
[49] AVSEC 10504 1.7.1 Actions by the Air Carrier, Operator, Entity 2
[50] AVSEC 10504 1.7.3 Actions by the Air Carrier, Operator, Entity 4
[51] https://www.bsi.bund.de/dok/6611684
[52] AVSEC 10504 1.7.1 Actions by the Air Carrier, Operator, Entity
[53] AVSEC 10504 1.7.2 Background 5

- Verteilung von Verantwortlichkeiten und Rollen
- etc.[54]

festgehalten und der jeweilige Einfluss auf die genannten Schutzziele

- Vertraulichkeit,
- Verfügbarkeit und
- Integrität

präzisiert.

Dabei sind auch die ermittelten kritischen informations- und kommunikationstechnischen Systeme und Daten von Drittanbietern zu berücksichtigen und aufzuführen, oder auf das entsprechende Sicherheitsprogramm des Drittanbieters zu verweisen.[55]

2.5 Überwachung – Monitoring

(1) Der Akteur bestimmt die erforderlichen Qualitätskontrollmaßnahmen zur Sicherstellung der Wirksamkeit der Risikobeurteilung[56] (siehe Abschnitt 2.3) und der Cybersicherheitsmaßnahmen[57] (siehe Abschnitt 2.4).

(2) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt:[58]

- Die durch den Akteur bestimmten Qualitätskontrollmaßnahmen[59] und
- deren jeweilige Zielrichtung

[54] AVSEC 10504 1.7.2 Background 3
[55] AVSEC 10504 1.7.1 Actions by the Air Carrier, Operator, Entity
[56] AVSEC 10504 1.7.3 Background 1
[57] AVSEC 10504 1.7.2 Actions by the Air Carrier, Operator, Entity 4
[58] AVSEC 10504 1.7.3 Background 1
[59] AVSEC 10504 1.7.2 Actions by the Air Carrier, Operator, Entity 4

2.6 Cybersicherheitsreaktionsplan – Cyber Incident Response Plan

(1) Der Akteur entwickelt und implementiert weitere Maßnahmen

- zur Erkennung von Cyberangriffen,
- zur Reaktion darauf und
- zu ihrer Bewältigung[60]

als Teil eines Cybersicherheitsreaktionsplans.[61]

Dieser Plan beschreibt - für den Fall der Unzuverlässigkeit oder Nichtverfügbarkeit von kritischen informations- und kommunikationstechnischen Systemen und Daten - unter anderem den Beitrag der zuständigen Personen für

- IT-Technologie,
- juristische Angelegenheiten,
- Instandhaltung und
- Öffentlichkeitsarbeit.[62]

(2) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt:

Maßnahmen, welche

- der Erkennung von Cyberangriffen,
- der Reaktion darauf und
- ihrer Bewältigung

dienen.[63]

[60] DVO (EU) 2015/1998 Anhang 1.7.2
[61] AVSEC 10504 1.7.3 Background 5
[62] AVSEC 10504 1.7.3 Background 5
[63] DVO (EU) 2015/1998 Anhang 1.7.2

3 Personalangelegenheiten (DVO 2015/1998 Anhang Punkt 11.1.2 & 11.2.8)

3.1 Zuverlässigkeitsüberprüfung

(1) Die folgenden Personengruppen sind zusätzlich einer luftsicherheitsrechtlichen Zuverlässigkeitsüberprüfung nach § 7 LuftSiG zu unterziehen:

(a) Personen, die Administrator-Rechte zu den ermittelten, für die Zivilluftfahrt genutzten, kritischen informations- und kommunikationstechnischen Systemen und Daten haben.[64]
(b) Personen, die unbeaufsichtigten und unbeschränkten Zugang zu den ermittelten, für die Zivilluftfahrt genutzten, kritischen informations- und kommunikationstechnischen Systemen und Daten haben. [65]
(c) Personen, die im Rahmen der Risikobewertung ermittelt wurden. [66]

(2) Externes Personal, das nur

- unregelmäßig,
- kurzfristig oder
- nicht durchgängig

Zugriff auf die kritischen informations- und kommunikationstechnischen Systeme und Daten hat, benötigt keine Zuverlässigkeitsüberprüfung, wenn es durch eine

- ihr zumindest gleichgestellte interne Person,
- mit abgeschlossener Zuverlässigkeitsüberprüfung und
- entsprechender IT-Qualifikation

durchgängig begleitet wird.

(3) Die folgenden Informationen werden im vorzulegenden (Luft-)Sicherheitsprogramm oder in einem darin referenzierten und bereitzustellenden Dokument hinterlegt:
Angabe des Verfahrens für die Einstellung und Überprüfung des Personals, einschließlich der verschiedenen Arten von Zuverlässigkeitsüberprüfungen und der Vorbeschäftigungsprüfungen.[67]

3.2 Eignung

Der Akteur stellt sicher, dass die Personen, welche die Maßnahmen nach Kapitel 2 umsetzen, über die erforderlichen Fähigkeiten und Fertigkeiten verfügen[68] und frühzeitig funktionsangemessen nach dem Grundsatz *„Kenntnis nur, wenn nötig“* über Cyberrisiken informiert werden.[69]

3.3 Schulung

Alle Mitarbeitenden müssen regelmäßig über neue Richtlinien und Verfahren informiert werden.[70]

Bei der Wissensvermittlung ist nach dem Grundsatz *„Kenntnis nur, wenn nötig“* vorzugehen.[71]

[64] DVO (EU) 2015/1998 Anhang 11.1.2 c)
[65] DVO (EU) 2015/1998 Anhang 11.1.2 c)
[66] DVO (EU) 2015/1998 Anhang 11.1.2 c)
[67] AVSEC 10504 11.1.2 Actions by the Air Carrier, Operator, Entity 1
[68] AVSEC 10504 11.2.8. Background 2
[69] AVSEC 10504 11.2.8. Background 3
[70] AVSEC 10504 11.2.8. Background 8
[71] DVO (EU) 2015/1998 Anhang 11.2.8.1

3.3.1 Personengruppen

Zur funktionsangemessenen Bestimmung der Schulungserfordernisse sollten die internen und externen Mitarbeitenden entsprechenden Personengruppen zugeordnet werden. Ist dabei eine Person auf Grundlage ihrer Tätigkeiten mehreren Personengruppen zuzuordnen, ist die Personengruppe mit der höchsten Anzahl an nötigen Schulungsinhalten maßgeblich.

3.3.1.1 Personen, die indirekten Einfluss auf kritische informations- und kommunikationstechnische Systeme und Daten haben.

Personengruppe a)

Personen, die keine (kritischen) Systeme betreiben oder Daten nutzen, in Ihrer Position jedoch Verletzungen der Cybersicherheit beobachten oder verursachen können, z. B. physische Manipulation der Geräte.[72]

3.3.1.2 Personen, die direkten Einfluss auf kritische informations- und kommunikationstechnische Systeme und Daten haben

Personengruppe b)

Personen, die kritische informations- und kommunikationstechnische Systeme und Daten nutzen und kontrollieren. Hierzu zählen u. a. Personen,

- die Sicherheitskontrollen durchführen[73]
- welche diejenigen unmittelbar überwachen, die eine Sicherheitskontrolle durchführen[74]
- die vernetzte Technologien nutzen, jedoch nicht über Administratorrechte zur Änderung (kritischer) informations- und kommunikationstechnische Systeme und Daten verfügen[75]

Personengruppe c)

Personen, für die Cybersicherheit zum Tätigkeitsprofil gehört. Hierzu zählen u. a. Personen,

- deren Tätigkeitsprofil dem eines Sicherheitsmanagers entspricht[76]
- die Administrator-Rechte haben[77]

Personen, die hauptsächlich mit Cybersicherheitsaufgaben betraut sind.[78]

Geschäftsführung, wenn erforderlich.

3.3.2 Schulungsthemen

Die Zuordnung der verpflichtenden Schulungsthemen zu den jeweiligen Personengruppen ist dem Dokument *„Grundsätze zur Umsetzung von Maßnahmen zum Schutz von kritischen informations- und kommunikationstechnischen Systemen und Daten in der Luftsicherheit gemäß dem Anhang der Durchführungsverordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit im Zuständigkeitsbereich des*

[72] AVSEC 10504 11.2.8. Background 7
[73] AVSEC 10504 11.2.8. Background 10
[74] AVSEC 10504 11.2.8. Background 10
[75] AVSEC 10504 11.2.8. Background 10
[76] AVSEC 10504 11.2.8. Background 10
[77] DVO (EU) 2015/1998 Anhang 11.1.2 c)
[78] AVSEC 10504 11.2.8. Background 7

Bundesministeriums des Innern und für Heimat (§§ 5 und 8 LuftSiG)" [79] (S. 15) zu entnehmen. Die Aufstellung der Schulungsthemen muss um den eigenen spezifischen Bedarf erweitert werden.

Zur Festlegung der Schulungsthemen ist die folgende Zuordnung der Personengruppen anzuwenden:

Schulungsthemen	**Personengruppe**		
	a)	b)	c)
Cyber Security Awareness	Ja	Ja	Ja
Anwenderschulung für Fachanwendungen	Nein	Ja	nach Erfordernis
Datensicherheit	Nein	nach Erfordernis	nach Erfordernis
Vorfallsbehandlung	Nein	nach Erfordernis	nach Erfordernis
Netzwerksicherheit	Nein	nach Erfordernis	nach Erfordernis
Malware	Nein	nach Erfordernis	nach Erfordernis
Sicherheitskonfiguration	Nein	nach Erfordernis	nach Erfordernis
Erweiterte Cyber Security Awareness	Nein	nach Erfordernis	nach Erfordernis
Hacking	Nein	nach Erfordernis	nach Erfordernis
Digitale Forensik	Nein	Nein	nach Erfordernis
Einhaltung von Vorschriften und Standards	Nein	nach Erfordernis	nach Erfordernis
Penetration Testing	Nein	nach Erfordernis	nach Erfordernis
Anwendungsentwicklung	Nein	nach Erfordernis	nach Erfordernis

Die detaillierten Schulungsinhalte zu den einzelnen Schulungsthemen werden in der jeweils aktuellen Fassung auf der Homepage des BSI für den Bereich Luftsicherheit[80] zur Verfügung gestellt.[81]

3.3.3 Durchführung von Schulungen

Die Ausbildenden müssen nicht über ein Ausbilderzertifikat verfügen.[82]

Die Ausbildenden müssen über tätigkeitsbezogene Kompetenzen und Erfahrungen verfügen.[83] Eine Personenzertifizierung mit Bezug zu ISO27001 (z. B. „Security Officer"), IT-Grundschutz (z. B. „IT-Grundschutzpraktiker") oder vergleichbare Zertifizierungen können ein Beleg für tätigkeitsbezogene Kompetenzen sein. Eine Genehmigung dieser Kompetenzen und Erfahrungen durch das Luftfahrt-Bundesamt ist nicht vorgesehen.

Die Schulungs- und Fortbildungsmaßnahmen können computergestützt erfolgen.[84] Eine Genehmigung dieser computergestützten Schulungen oder Fortbildungen durch das Luftfahrt-Bundesamt ist nicht vorgesehen.[85]

79 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/LuSi/LuftSiG_Hauptdokument.pdf?__blob=publicationFile&v=8

80 https://www.bsi.bund.de/dok/luftsicherheit-grundsaetze

81 AVSEC 10504 11.2.8. Background 5 (a)

82 § 19 (1) LuftSiSchulV

83 § 4 (1) S. 2 und § 5 (1) LuftSiSchulV i. V. m. § 19 (1) LuftSiSchulV

84 § 4 (1) und § 5 (1) LuftSiSchulV

85 § 5 (1) LuftSiSchulV i. V. m. § 9 (4) Nr. 1 LuftSiSchulV

3.3.4 Dokumentation

Die Schulungsthemen gemäß Abschnitt 3.3.2 sind für jedes Tätigkeitsprofil – je nach Zuordnung zu den Personengruppen – festzulegen und im (L)SP zu dokumentieren.[86]

Die Dokumentation der durchgeführten Schulungs- und Fortbildungsmaßnahmen ist für alle teilnehmenden Personen zu pflegen, aufzubewahren und auf dem neuesten Stand zu halten.[87]

[86] AVSEC 10504 11.2.8. Background 6
[87] AVSEC 10504 11.2.8. Background 19

Anhang B Risikomanagement

B.2.2 Ermittlung kritischer Informations- und kommunikationstechnischer Systeme und Daten

Ein prozessorientierter Ansatz zur Ermittlung der kritischen Informations- und kommunikationstechnischen Systeme und Daten (zu Abschnitt 2.2 (1)) wäre bspw. eine umfängliche Unterteilung ausgehend von der zentralen Dienstleistung zur Erstellung einer Übersicht der kritischen informations- und kommunikationstechnische Systeme und Daten:

Dienstleistung[88]	Reise					
(Unter-)Funktion[89]	…					
Perspektive[90]	Passagier/in					…
Ort[91]	Landseite			Luftseite	…	…
Phase[92]	vor dem Flug	Start	…	…		
Systeme	System A	Daten B	…	…		
Verantwortung[93]	Luftfahrtunternehmen	Externer Dienstleister	…	…		
kritisch	**Ja**	**Nein**	…	…		

[88] AVSEC 10504 1.7.2 Background 9
[89] AVSEC 10504 1.7.2 Background 9
[90] AVSEC 10504 1.7.2 Background 12
[91] AVSEC 10504 1.7.2 Background 12
[92] AVSEC 10504 1.7.2 Background 12
[93] AVSEC 10504 1.7.2 Background 10

Die folgende Liste stellt eine beispielhafte, nicht abschließende Aufzählung kritischer informations- und kommunikationstechnischen Systeme und Daten dar[94] [95] [96], die durch weitere, im Rahmen unternehmensinterner Ermittlungen identifizierte KIKS, ergänzt werden kann.

(1) Erkennungssysteme und Sprengstoff-Erkennungssysteme, unabhängig davon, ob sie vernetzt oder als allein operierende Geräte betrieben werden, wie z. B.:

- EDS, ETD, LED
- WTMD, Body Scanner,
- X-Ray
- Technik zur Fahrzeuguntersuchung

(2) Datenbanken und Archive (inkl. Zugriffsmöglichkeiten) mit Informationen zu

- reglementierten Beauftragten, bekannten Versendern, reglementierten und bekannten Lieferanten, anderen amtlich anerkannten oder benannten Stellen, die zur sicheren Lieferkette gehören (Union database)
- Flughafenidentifikationskarten
- Dateien zur Einstellungsüberprüfung, beschäftigungsbezogener Überprüfungen und Zuverlässigkeitsüberprüfung;
- Personaldateien zu Sicherheitsschulungen und Nachweisen

(3) Überwachungssysteme, wie z. B.:

- Kameraüberwachung
- Perimeter-Intrusion-Detection
- Alarm- und Alarmüberwachungssysteme
- Zugangskontrollen für Personen, die keine Fluggäste sind, einschließlich elektronischer Gates und sonstiger Eingänge

(4) Sonstige kritische informations- und kommunikationstechnischen Systeme und Daten, wie z. B.:

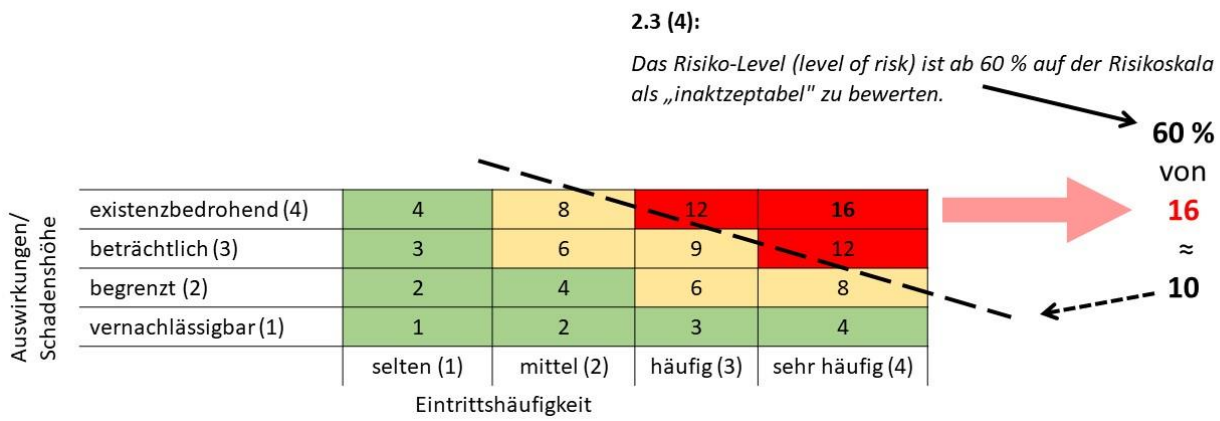
- Passagier- und Gepäckabgleichsystem; Airport und Online check-in
- Lesegeräte für elektronische Pässe, Personalausweise und Bordkarten
- Externe Netzwerkverbindungen zu kritischen informations- und kommunikationstechnischen Systemen und Daten Dritter
- NCASP, (L)SP
- Sicherheitsdaten, Verfahren, Handbücher

[94] AVSEC 10504 1.7.2 Background 8
[95] AVSEC 10504 1.7.3 Background 4 (k)
[96] AVSEC 10904b

B.2.3 Risikobeurteilung - Risk assessment

Die folgenden beiden Beispiele illustrieren zu den Abschnitten 2.3 (4) und 2.4 (3), wie anhand der durch den Akteur zu erstellenden qualitativen Risikomatrix die Risiken ermittelt werden, zu denen Maßnahmen ergriffen/ausgestaltet werden müssen, sodass durch deren Umsetzung das Risiko-Level nicht mehr überschritten wird.

Risikomatrix Beispiel 1:



Risikomatrix Beispiel 2: