BDLI Fachausschuss Cybersicherheit

GUIDELINE FÜR DIE SECURITY UND SAFETY IN DER LUFTFAHRT

BDLI Bundesverband der Deutschen Luft- und Raumfahrtindustrie e. V. (BDLI)

Online lesen

BDLI Fachausschuss Cybersicherheit

GUIDELINE FÜR DIE SECURITY UND SAFETY IN DER LUFTFAHRT

Online lesen

INHALT

IHR ANSPRECHPARTNER IM BDLI

UAS, CYBERSICHERHEIT
Robert Friebe, Referent
friebe@bdli.de

1. EINLEITUNG

Safety: „Beinhaltet den Zustand "Frei von Risiken und Gefahren zu sein" und beschreibt die Mittel und Maßnahmen diesen Zustand zu erreichen und zu sichern. Kurz: „ Sicherheit & Schutz des System und der Nutzer".

Cyber Security: „Der Schutz von Informationssystemen vor Angriffen, Störungen oder Fehlleitung der wesentlichen Funktionen bzw. Services die diese Systeme bieten". Kurz: Sicherheit & Schutz der Information."

Worum geht es in dem Dokument?
Das Handout hat zum Ziel einen groben Abriss zu erstellen was Unternehmen zu kommenden Cyber Security Anforderungen in der Luftfahrt beachten müssen. Die Hilfestellung soll Klarheit bzgl. der Begrifflichkeit Safety und Security geben und externe Stellen auflisten, bei denen weitere Informationen eingeholt werden können. Der Schwerpunkt wird hierbei auf die Entwicklung, Produktion und Wartung von Produkten für die Luftfahrt gelegt und soll damit Entwicklungs- und Produktionsbetriebe gleichermaßen ansprechen. Als Grundlage wird hierfür die Veröffentlichung des Vorschlages NPA 2019-01"Aircraft Cyber Security" durch die EASA genutzt.

Zielgruppe
Dieses Dokument richtet sich an IT-Verantwortliche bei Herstellern und Zulieferern (BDLI-Mitgliedsunternehmen) mit dem Fokus auf KMU (Klein- und Mittelständische Unternehmen).

Die folgenden Checklisten stellen eine Arbeitshilfe sowohl zum Prüfen der „Cyber-Readiness" (Abhaken der Checkliste), als auch dem Sicherstellen, dass im Incidentfall geeignete Maßnahmen ergriffen werden.

1.1. ANFORDERUNGEN AN DAS MITARBEITER-KNOW HOW

Bei der Aufnahme des Ist-Standes (meist im Verbund mit einem Risk Assess-

ment) wird häufig festgestellt, dass die IT-Sicherheitskultur nicht so gelebt wird, wie es optimalerweise sein sollte. Oftmals zeigt sich dies in einem falschen Umgang mit sensiblen Geräten oder in mangelnder Wahrnehmung und mangelndem Wissen über gängige Gefahren und Risiken. Dabei ist es unerheblich, mit welchem Aufgabengebiet die Mitarbeiter betraut sind, denn eine nachhaltige und gesunde IT-Sicherheitskultur muss sowohl von den Anwendern, dem IT-Fachpersonal , als auch vom Management gelebt werden.

Ein weiteres Problem ist, dass es kaum Personal gibt, das an der Schnittstelle zwischen Informatik und Luftfahrt ausgebildet ist. Im klassischen ingenieurswissenschaftlichen Studium werden bestenfalls die Grundlagen des Programmierens beigebracht, jedoch spielt Cybersicherheit kaum eine Rolle. Andererseits haben ExpertInnen der Cybersicherheit mit den Prozessen/ Einschränkungen von sicherheitskritischen LFZ wenig Erfahrung.

Durch Zielgruppen-spezifische IT-Security Awareness-Maßnahmen kann eine solche IT-Sicherheitskultur in den Zieldimensionen Wahrnehmung, Wissen (z.B. über gängige Angriffsvektoren) und regelkonformen Verhalten intensiviert und gefördert werden.

Begleitend ist es ratsam, im Falle nicht mehr zeitgemäßer Unternehmens-Policies neue Richtlinien zu entwickeln und diese über verschiedene Medien und Methoden an die Mitarbeiter zu transportieren. Hierzu zählen beispielsweise interaktive Vorträge, Trainings, Serious (Awareness) Games sowie Übungen.

Folgende Fortbildungen befinden sich bereits auf dem Markt, um in angemessener Zeit Mitarbeiter effizient im Bereich IT-Sicherheit fachübergreifend zu schulen.

1.2. SCHULUNGEN (IT-SECURITY)

Implementing and Auditing the Critical Security Controls - In-Depth (**SANS**-Institute)
Defensible Security Architecture and Engineering **(SANS)**
Intrusion Detection In-Depth **(SANS)**
IT-Grundschutz-Schulungen **(BSI)**
Informationssicherheit nach ISO/IEC 27000 Reihe **(TÜV)**
Zertifizierungen (IT-Security)
CISSP – Certified Information Systems Security Professional (**(ISC)²**)
(CompTIA) Advanced Security Practitioner (CASP)

Die Teilnehmer erlangen dadurch Wissen über den richtigen Umgang mit sensiblen Geräten wie „mobile Devices“. Durch einen bewussteren Umgang,

hinsichtlich deren Sicherheitsaspekte, schützen sie die IT und IT-Systeme besser und gleichzeitig die Vermögenswerte der Organisation.

Bezogen auf das Erkennen von Risiken lernen die Teilnehmer während der Awareness-Maßnahmen, welche die richtigen Abwehrmaßnahmen für den jeweiligen Fall sind. Damit lassen sich eventuelle Schadensfälle in der IT wie u.a. Datenverlust vorbeugen.

Die Mitarbeiter sind nach der Durchführung einer IT-Notfallübung in der Lage, Sicherheitsvorfälle schneller zu erkennen, was zu einer besseren Reaktion auf Sicherheitsvorfälle führt und somit zu routinierterem Handeln und gesteigerter Handlungssicherheit.

Neben den Awareness Trainings können außerdem Business Continuity Trainings dabei unterstützen, Sicherheitsmaßnahmen in der Praxis zu leben. Die Organisation sollte zuvor Prozesse, Verfahren und Maßnahmen festlegen, dokumentieren und umsetzen , um das erforderliche Niveau an Informationssicherheit in einer widrigen Situation aufrechterhalten zu können. Dadurch verbessern sich wiederum die Fähigkeiten im Cyber Incident Handling hinsichtlich Lagebeurteilung, Entwicklung von Handlungsoptionen, Geschäftsfortführung sowie Wiederanlauf und Nachbereitung.

2. VORGEHENSWEISE, PRODUKTE UND LÖSUNGEN

2.1. SECURITY MEETS SAFETY

Für die Entwicklung von Produkten/ Komponenten wird ein hohes Augenmerk auf Sicherheit (Safety) gelegt. Dies wird durch diverse Entwicklung-Anweisungen (z.B. ARP 4761 Methoden zur Safety Analyse für Luftfahrtzulassungen, RTCA-DO 178C/ DO-254 Vorgehen für Software Entwicklung von Sicherheit kritischer Software und Hardware). Bisher wurde für sicherheitskritische der nachfolgende Entwicklungsprozess empfohlen (siehe Abbildung 1).

Durch die wachsende Zahl an Informationen ergeben sich neue Bedrohungsszenarien, welche die Sicherheit von Luftfahrt Produkten gefährden. Diesen Tatbestand hat die EASA (European Aviation Safety Agency) erkannt und fordert für zukünftige Entwicklung den Aspekt der Informationssicherheit (Cyber Security) einen entsprechenden Stellenwert einzuräumen. Durch diese Anforderungen ergibt sich eine Ergänzung des Entwicklungsprozesses entsprechend der Abbildung 2.

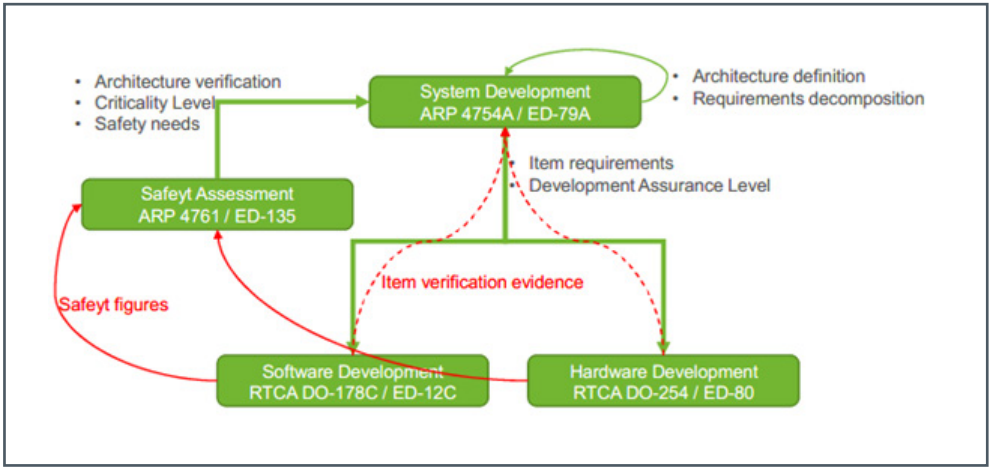

Abbildung 1 Klassische Entwicklungs-Empfehlungen

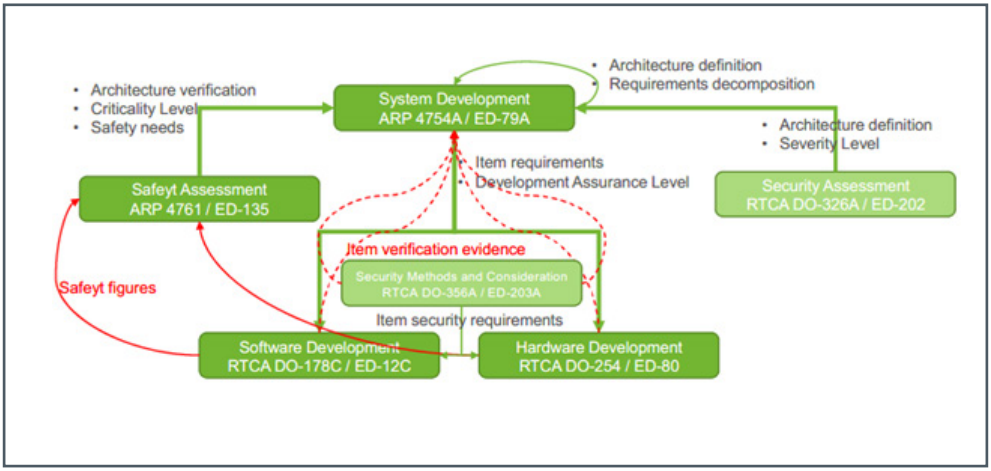

Abbildung 2 Entwicklungsprozesse inklusive Informationssicherheit

Die erweiterten Anforderungen bzgl. Informationssicherheit dienen primär dem Zweck die Sicherheit in der Luftfahrt weiterhin zu gewährleisten, d.h. hohe operationelle Sicherheit „Safety“ ist weiterhin die Prämisse der Luftfahrt und „fehlende“ Informationssicherheit muss als ein Bedrohungsszenario im Hinblick auf operationelle Sicherheit verstanden werden.

Für Entwicklungs-, Instandsetzungen und Service Anbieter im Umfeld der von kritischen Luftfahrtsystemen ergeben sich somit neue Anforderungen im Hinblick auf Informationssicherheit, welche sich in folgende aufgliedern:

1. Sicherstellen von Informationssicherheit in der Unternehmenskultur und Organisation: Es gibt zwischen der rasanten Entwicklung von Informationssystemen und den langwierigen Entwicklung- , Zulassungs- und Betriebsdauern von LFZ und Infrastruktur ein Spannungsfeld. Daher ist es sehr schwierig, Betriebssicherheitsarchitekturen/ +Mechanismen zu entwickeln, die noch in 50 Jahren funktionieren und noch entsprechenden Schutz bieten. Durch einen entsprechenden Update-Prozess kann dies zwar verbessert werden, andererseits ergeben sich durch die Tests im Rahmen der Zulassung Verzögerungen, wodurch nicht mit der gleichen Geschwindigkeit wie bei Standard-IT Systemen auf neu erkannte Bedrohungen reagiert werden kann.

2. Erweiterung der Entwicklungskompetenzen im Hinblick auf Informationssicherheit: Durch diese erweiterten Anforderungen an Informationssicherheit zeigen sich nachfolgende Standards für Luftfahrtunternehmen von essentiellem Interesse:

2.2. ENTWICKLUNGSSTANDARDS UND GÜTESIEGEL

Organisationseinheit:
ISO/ IEC 27000:2018: “Information technology – Security techniques – Information security managementsystems„; 2018 [Management System –Security Environment].

Diese Internationale Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Entwicklungsstandards:
D-201: "Aeronautical Information System Security (AISS) Framework Guidance“; 2015 [WhyandWho]
DO-326A/ED-202A: "Airworthiness Security Process Specification"; original – 2010, revA – 2014 [What]
DO-356A/ED-203A: "Airworthiness Security Methods& Considerations“; original – 2014/2015, rev A –2018 [HOW]
DO-355/ED-204: "Information Security Guidance for Continuing Airworthiness“; 2014 [ThenWhat]
Sofern das Thema Informationssicherheit „neu“ ist (Als Unternehmen besitzt man kein Prüfsiegel bzgl. Informationssicherheit) wird empfohlen sich im Bereich der Informationssicherheit durch externe Stellen beraten zu lassen.
ARINC Technical Report 811, “Commercial Aircraft Information Security Concepts of Operation and Process Framework”, July 2005

ARINC 835: GUIDANCE FOR SECURITY OF LOADABLE SOFTWARE PARTS USING DIGITAL SIGNATURES

AEEC Technical Application Bulletin ABN-35A, “Considerations for the Incorporation of Cyber Security in the Development of Industry Standards”, February 2011

ATA Spec 42: Aviation Industry Standards for Digital Information Security: Spec 42 liefert Empfehlungen zu standartisierten Methoden um ein angemessenes Level of Security in einer Anwendung zu erreichen, die auf digitaler Identität basiert

EN 16495:2014 ist Teil des WP of CEN/TC 377 ‘Air Traffic Management’. Dieser Europäische Standard definiert Guidelines und generelle Prinzipien für die Implementierung eines Informationssicherheits-Management Systems in Organisationen welche den Betrieb ziviler Luftfahrt unterstützen.

ENISA TP-07-16-070-EN-N 'Securing smart airports'

Regulation (EC) No. 300/2008 - Common rules and basic standards on aviation security

Implementing Regulation (EU) No. 2015/2426 - Amending Reg (EU) 2015/1998 - regarding recognition of 3rd countries

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS 204A

SECURITY ACREDITATION OF ATM SYSTEMS ED205


Checklist

Gütesiegel für Organisationen:
Nachfolgende Liste führt Gütesiegel und anerkannte Prüfstellen bzgl. Informationssicherheit auf:

ISO/ IEC 27000:2018 <https://www.iso27001security.com/html/27001.html>
- Unternehmen mit einem ISO/ IEC 27000:2018 Prüfsiegel besitzen einen strukturierten Prozess für Informationssicherheits-Managementsystems und werden von unabhängigen Stellen (z.B. DEKRA) in regelmäßigen Abständen (1mal/ Jahr) auditiert.
- Das bestehende ISMS kann zertifiziert werden. Dieses wird dann jährlich auditiert und alle 3 Jahre rezertifiziert.
- Anwendbarkeit: Für alle Unternehmen die direkt oder indirekt mit der Entwicklung/ Fertigung und Wartung von Luftfahrtgeräten beschäftigt ist

Trainingsanbieter bzgl. Informationssicherheit in der Entwicklung von sicherheitskritischen Geräten:

- UROCAE (https://www.eurocae.net/)

- AFUZION (https://afuzion.com/training/)

3. CHECKLISTEN

Die folgenden drei Cyber Security Checklisten orientieren sich an drei unterschiedlichen Phasen. Zuerst die Checkliste für „secured-by-Design“, die bereits bei der Entwicklung von Hard- und Software ansetzt. Dann die zweite Checkliste für das Einleiten geeigneter Präventiv-Maßnahmen und die dritte Checkliste, die auf die zu ergreifenden Maßnahmen im Krisenfall fokussiert.

3.1. TECHNISCHE CHECKLISTE

☐ Vorbereitung

Die anwendbaren Vorgaben zur Cyber Security sind definiert

☐ Sicheres Design

Beim Entwurf eines neuen Produktes sollten insbesondere Aspekte berücksichtigt werden, die die künftige Wartung des Produktes vereinfachen. Dies bezieht sich insbesondere auf die Notwendigkeit von Re-Validierung nach Änderungen.

- Es sind Entwurfsmuster bzw. Regeln bekannt, die der Kapselung von Cyber Security Funktionen bzw. Komponenten dienen
- Die Gesamtarchitektur ist so ausgelegt, dass spätere Änderungen (updates) leicht vorgenommen werden können

☐ Sichere Implementierung

Für die Implementierung sollten Vorgaben gemacht werden, die für ein sicheres Produkt zuträglich sind und deren Einhaltung auch mit vertretbarem Aufwand verfolgt werden kann. Dazu gehören Implementierungs-Richtlinien, die mit Hilfe von statischen Analyse Werkzeugen überwacht werden können. Weitere Elemente wie konsequente Fehlerbehandlung, Vermeidung von unsicheren Funktionen, etc bedürfen einer hinreichenden Schulung vom Personal und können durch unabhängige Reviews sichergestellt werden.

- Implementierungs-Richtlinien sind definiert
- Es gibt Werkzeuge zur Überwachung der Richtlinien
- Mitarbeiter sind geschult in Bezug auf Sicherheits-Beurteilungen und kennen bekannte Schwachstellen (z.B. durch firmeninterne Know How Datenbanken)

☐ Im Kontext der Implementierung ist auch der angemessene Einsatz von Werkzeugen von Dritten sicherzustellen. Wo Fremdwerkzeuge eingesetzt werden, sollte sichergestellt sein:

- Das Werkzeug stammt aus vertrauenswürdiger Quelle
- Funktionen aus dritter Hand sind gut gekapselt / abstrahiert
- Die Werkzeuge werden aktiv gewartet ,gepflegt und genügen den aktuellen Sicherheitsstandards (z.B. Sicherheits Patches)

☐ Testing

Für die (Re-) Validierung der Produkte sind Testverfahren zu bevorzugen, die in hohem Maße automatisiert sind. Zwar sind automatisierte Tests mit relativ hohem initialen Aufwand verbunden. Im Gegenzug ist eine Revalidierung einer neuen SW Version nun kurzfristig und mit geringem Aufwand durchführbar.

- Für die geplante Entwicklung sind möglichst automatisierte Tests eingeplant
- Die Tests umfassen dabei alle notwendigen Testebenen wie beispielsweise Geräte, Hardware und Software (Unit Tests, Integrationstests, etc)
- Für besonders sicherheitskritische Produkte sollten sogenannte Penetration Tests in Erwägung gezogen werden

3.2. CHECKLISTE FÜR PRÄVENTIVE MASSNAHMEN

Indikation der unternehmensinternen Informationssicherheit kann mit der nachfolgenden Checkliste durch die DEKRA durchgeführt werden:

Eine weitere Quelle ist die internationale Empfehlung der ECCSA (European Centre for Cyber Security in Aviation). Die folgende Checkliste enthält zusammengefasst die wichtigsten Empfehlungen aus beiden Quellen.

- [ ] Cyber Security Trainings- und Simulationssysteme werden genutzt
- [ ] Sie besitzen ein dokumentiertes Risikobewertungsverfahren
- [ ] Sie verfügen über eine umfassende Dokumentation zum Risikobeurteilungsprozess und Risikobehandlungsprozess/-plan
- [ ] Sie besitzen alle Aufzeichnungen und Ergebnisse von Risk Assessments bzw. Risikoanalysen
- [ ] Sie haben alle Aufzeichnungen und Ergebnisse von Risikobehandlungen dokumentiert
- [ ] Sie haben alle Sicherheitsziele für Ihr Unternehmen und Stakeholder definiert.
- [ ] Sie verfügen über einen Kommunikationsplan bzw. -matrix
- [ ] Es existiert eine Dokumentation aller Datenkommunikation im Unternehmen und nach extern
- [ ] Netzwerk- und Informationssysteme sind geschützt (Firewall, Datendioden, etc)
- [ ] Sie schützen und überwachen Ihre Lieferketten
- [ ] Es ist sichergestellt, dass Schwachstellen in vorhandenen COTS-Systemen (Commercial of the shelf) analysiert und minimiert werden
- [ ] Ein präventives „Cyber Secuity Monitoring“ über ein internes SOC (Security Operation Center) oder als Managed Service wird zur Früherkennung von Angriffen genutzt.
- [ ] Interne Abstimmungsprozesse sind geregelt:
  - Management
  - Rechtsabteilung
  - IT-Sicherheitsbeauftragter
  - Datenschutzbeauftragter
  - Pressestelle
  - Betriebsrat
- [ ] Rechtliche Zuständigkeit für Strafanzeigenerstattung sind geklärt.

3.3 CHECKLISTE FÜR MASSNAHMEN IM KRISENFALL

- [ ] Betroffene Systeme im laufenden Betrieb vom Netzwerk isolieren. - Nicht ausschalten!
- [ ] Möglichst genaue Vorfallsbeschreibung verfassen.
- [ ] Weiteres Vorgehen mit den Ermittlungsbehörden besprechen.
- [ ] Daten sichern und bereitstellen, beispielsweise Logfiles (mit Unterstützung der Ermittlungsbehörden).

Reaktionen koordinieren:

- [ ] Verhaltens- und Kommunikationsrichtlinien für Mitarbeiter und Führungskräfte erstellen. Ermittlungsbehörden Zutritt zum Gebäude sowie Zugang und Zugriff zu den betroffenen IT-Systemen gewähren.
- [ ] Strategie für Reputations und Öffentlichkeitsmanagement erarbeiten, ggf. in Abstimmung mit den Ermittlungsbehörden.
- [ ] Meldung von Schwächen in der Informationssicherheit
- [ ] Sammeln von Beweismaterial
- [ ] Planung zur Aufrechterhaltung der Informationssicherheit
- [ ] Umsetzung der Aufrechterhaltung der Informationssicherheit

NOTIZEN

IMPRESSUM:

Bildnachweis:
Adobe Stock, Julia Baumgart

Herausgeber:
Bundesverband der Deutschen
Luft- und Raumfahrtindustrie e.V. (BDLI)

ATRIUM Friedrichstr. 60
10117 Berlin
+49 (0)30 206140-0
kontakt@bdli.de
www.bdli.de

Verantwortlich: Cornelia von Ammon
Layout: Katja Zehe

September 2020