UAVDACH
ASSOCIATION FOR UNMANNED AVIATION

IT-Grundschutz-Profil
für den Betrieb von UAS
Band 1: UAS-Betriebskategorie „Open (Offen)“

Inhalt

1. Einleitung

Der Betrieb von Unmanned Aircraft Systems (UAS) stellt neben den Anforderungen an die Flugsicherheit auch Anforderungen an die Informationssicherheit. Als fliegende Rechnerverbünde sind sie schutzbedürftig, denn korrumpierte Firmwareupdates, ein Ausfall der Kommunikationsinfrastruktur oder manipulierte Datenbanken können zu einem Fehlverhalten des Fahrzeugs führen und damit dieses zu einer Gefahr für Menschen und Umwelt werden lassen. Der Schutz von Daten und die sichere Kommunikation mit dem unternehmensinternen Netzwerk machen daher eine genauere Betrachtung in punkto Informationssicherheit erforderlich. Informationssicherheit bei UAS ist aus zwei Perspektiven zu betrachten: zum einen aus der Sicht des UAS als Teilnehmer am Luftverkehr und zum anderen aus der Sicht des mobilen Endgeräts und Datenspeichers.

Grundsätzlich soll das vorliegende IT-Grundschutz-Profil den Beteiligten diese Bürde ab-nehmen und anhand einer Referenzarchitektur die wichtigen Fragen zur Informationssicherheit beim Betrieb von UAS klären. Insbesondere sollen folgende Fragen adressiert wer-den: Wie kann durch geeignete Maßnahmen der Informationssicherheit eine Beeinträchtigung des sicheren Flugbetriebs vermieden werden? Wie können Gefahren für ein verbundenes Netzwerk abgewendet werden? Die Aspekte im Bereich Datenschutz, wie die daten-schutzkonforme Datenerhebung für den Betrieb der Drohne und die Datenverarbeitung von Bilddaten aus der Luft, unterliegen den entsprechenden gesetzlichen Bestimmungen und sind nicht Gegenstand des IT-Grundschutzprofils.

Die Gründe sich mit der Informationssicherheit beim Betrieb von UAS auseinanderzusetzen sind vielfältig. Die Wichtigsten dürften sein, Personen- und Sachschäden durch mangelhafte Informationssicherheit zu vermeiden. Dieses IT-Grundschutz-Profil ist dazu geeignet, Prozesse, die für die gebräuchliche IT-Landschaft etabliert wurden, auf den Betrieb von UAS zu übertragen. Dort, wo dies nicht möglich ist, wurden individuelle Bausteine entwickelt. Das IT-Grundschutz-Profil kann ferner als Element für eine Risikoanalyse zur Vorlage bei Luftfahrtbehörden dienen.

1.1 Formale Aspekte

Aspekt	Beschreibung
Titel	IT-Grundschutz-Profil für den Betrieb von UAS Band 1: UAS-Betriebskategorie "offen"
Autorenschaft	Jens Fehler (Mediator Consult) Kai Lothar John (GLVI) Marco Müller-ter Jung, LL.M. (Grant Thornton Rechtsanwaltsgesellschaft mbH) Harald Rossol (b.r.m. IT & Aerospace) Markus Rossol (b.r.m. IT & Aerospace) Corinna Schmitt (Universität der Bundeswehr München) Burkhard Wrenger (TH OWL)
Herausgeber	UAV DACH e.V.
Versionsstand	1.0
Revisionszyklus	Es wird nach Freigabe der Version 1.0 eine zwei-jährliche Überprüfung angestrebt.
Vertraulichkeit	Dieses Dokument darf in unveränderter Version weitergegeben werden.

Tabelle 1: Übersicht über formale Aspekte

1.2 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profils durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, so dass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

2. Management Summary

2.1.Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an alle Organisationen, Behörden und Unternehmen, in denen UAS im Rahmen der Betriebskategorie "offen" zum Einsatz kommen. Es ist insbesondere gedacht für die Verantwortlichen in der Geschäftsleitung und der IT-Administration, sowie jene Fachbereiche, in denen UAS eingesetzt werden.

2.2.Zielsetzung

Das IT-Grundschutz-Profil definiert Anforderungen im Sinne des IT-Grundschutzes, um die Absicherung der verarbeiteten Daten hinsichtlich deren Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen. Der Betrieb von UAS wird beispielhaft dargestellt durch die Prozesse

- GP1: Flugbetrieb mit den Teilprozessen
  - Startvorbereitungen,
  - Start,
  - Flug,
  - Landung,
  - Außerbetriebnahme.
- GP2: Wartung und Instandsetzung mit den Teilprozessen
  - Austausch oder Aktualisierung der mechanischen Antriebskomponenten,
  - Aktualisierung der Flugbetriebssoftware,
  - Aktualisierung aller weiteren Softwarekomponenten nach Herstellervorgabe,
  - Analyse der System-Dateien (Log-Dateien).

2.3.Aufgaben der Leitungsebene

Die Anwendung dieses IT-Grundschutz-Profils im Rahmen des Flugbetriebes mit UAS ist Teil einer Sicherheitskonzeption und kann als Element der Zulassung oder Genehmigung von Luftfahrtbetrieben nach den einschlägigen Richtlinien und Bestimmungen dienen.

Die Autorinnen und Autoren empfehlen, dass Organisationen, die UAS-Dienste in Anspruch nehmen wollen, das vorliegende IT-Grundschutz-Profil als Grundlage für die Beauftragung entsprechender Dienstleister verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.

3. Festlegung des Geltungsbereichs

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen des UAV DACH e.V. für UAS-Betreiber. Sie decken die Anforderungen der "Standard-Absicherung" des BSI-Standards 200-2 ab.

Die Umsetzung der Standard-Absicherung ist konform zur ISO 27001.

Die in diesem IT-Grundschutz-Profil dargestellten Anforderungen berücksichtigen auch Teile der Vorgaben der DSGVO, des BDSG, des TTDSG, des TMG, insbesondere § 13 TMG, und für U-Space-Service-Provider zusätzlich den Anhang III der Durchführungsverordnung 2021/664 für den U-Space.

Es wird darauf hingewiesen, dass zum Zeitpunkt der Veröffentlichung dieses IT-Grundschutz-Profils sämtliche EU-Cybersecurity-Zertifikate von ENISA (vgl. Art. 8, 48 ff der Verordnung EU 2019/881 (Cybersecurity Act)) noch immer im Aufbau sind. Dieses IT-Grundschutz-Profil ist daher auf eine Selbstimplementierung und bei Verfügbarkeit der Zertifikate auf eine Selbstbewertung der Konformität durch den Hersteller oder Verwender des UAS ausgelegt. Daher wäre im Rahmen der Einstufung Vertrauenswürdigkeit nach den europäischen Schemata[1] der ENISA gem. Art. 53 des Cybersecurity Acts höchstens eine Erreichung der Vertrauenswürdigkeitsstufe „niedrig“ möglich. Für die weiteren Stufen „mittel“ und „hoch“ wären hingegen Prüfungen durch akkreditierte unabhängige Dritte erforderlich.

[1] Drohnen dürften nach Art. 2 Nr. 12 Cybersecurity Act als ein **IKT-Produkt** einzustufen sein, jedenfalls aber – je nach Bauart der Drohne – die verbauten Komponenten (Video- und Fotokamera, Mikrofone, Netzwerkverbindung zu U-Space-Service-Providern, etc.). Es gilt das Schema **„Cybersecurity Certification: EUCC Scheme V1.1.1“** (im Aufbau), das IKT-Produkte behandelt, zu beachten. Ferner ist ggf. das Schema **„EUCS – Cloud Services Scheme“** zu beachten, sofern U-Space-Service-Provider als Cloud-Dienstleister i.S.d Art. 2 Nr. 13 Cybersecurity Act anzuse-hen sind.

4. Abgrenzung Informationsverbund

4.1. Bestandteile des Informationsverbunds

Zum Informationsverbund gehören alle Komponenten und Verfahren bei einem UAS-Betreiber, die für die Durchführung des Flugbetriebs einschließlich Wartung und Instandsetzung notwendig sind (siehe Referenzarchitektur, siehe Ziffer 5.).

4.2. Nicht berücksichtigte Objekte

Nicht berücksichtigt werden Komponenten, die nicht unmittelbar mit dem Flugbetrieb zusammenhängen, sowie Verfahren, die über den Flugbetrieb hinausgehen, wie z.B. Auftrags-wesen, Rechnungsstellung, usw.

Nutzer von UAS-Diensten sollten das vorliegende IT-Grundschutz-Profil als Grundlage für die Auswahl entsprechender Dienstleister verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.

5. Referenzarchitektur

Der vom IT-Grundschutz-Profil betrachtete Informationsverbund beinhaltet alle wesentlichen mobilen und stationären Objekte des Unmanned Aircraft Systems (UAS), die für den Betrieb im Rahmen der nachfolgend dargestellten Geschäftsprozesse essenziell sind. Eine schematische Darstellung des Informationsverbunds ist Abbildung 1 zu entnehmen.

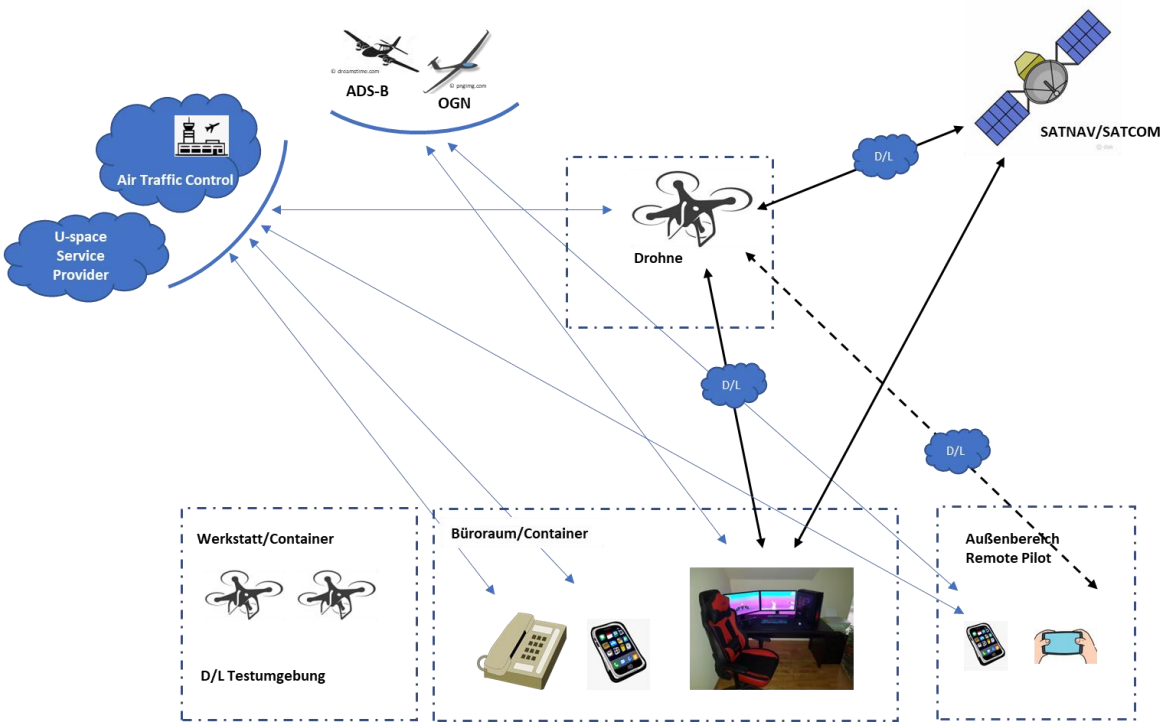

Abbildung 1: Schematische Darstellung der Referenzarchitektur[2]

Der Schutzbedarf bezieht sich auf die dargestellten Elemente und Komponenten, insbesondere Gebäude und Räume, Computernetze und Kommunikation, IT-Systeme und Geschäftsprozesse/Anwendungen. Es findet eine Kommunikation zwischen unterschiedlichen Endgeräten statt, beispielsweise Desktop-Rechner, Laptops, Tablet sowie Steuerrechnern. Dafür werden unterschiedliche Kommunikationsverfahren verwendet. Die Sicherheitsanforderungen sind von jeder Institution individuell zu prüfen.

5.1. Geschäftsprozesse und Anwendungen

Das betrachtete IT-Grundschutz-Profil bezieht sich auf die Geschäftsprozesse

- GP1: Flugbetrieb
- GP2: Wartung und Instandsetzung

Diese Geschäftsprozesse stehen exemplarisch für unterschiedliche Teilaspekte und Schutzziele und können durch die konkreten Geschäftsprozesse der Organisation ersetzt werden.

[2] Aktuelle Version der Grafik kann über folgenden Link bezogen werden: https://uavdach.sharepoint.com/:p:/r/teams/FGIT-Sicherheit/Freigegebene Dokumente/IT-Grundschutzprofil/20220301-Drohnen-IT-GSProfil_v2.pptx?d=w397d4f3e1d334cda915ed31e179d116c&csf=1&web=1&e=LWoNAc

GP1 beinhaltet die Inbetriebnahme des UAS, dessen Start, den Flug, die Landung, die anschließende Außerbetriebnahme, sowie mit dem Flug unmittelbar verbundene Tätigkeiten wie z.B. die Flugvorbereitung.

Für GP1 sind daher der Aufbau des UAS am Startort oder in dessen Nähe, die vor dem Start durchzuführenden mechanischen, elektrischen und elektronischen Tests und Selbsttests sowie die kommunikationstechnische Verbindung zwischen den Teilkomponenten des UAS zu berücksichtigen. Nach dem Start sind weitere Tests des UAS und seiner Nutzlast, die automatische oder manuelle Überwachung des Flugkorridors und des Systemzustands sowie des Flugfortschritts zu berücksichtigen. Nach der Landung erfolgen weitere (Selbst-)Tests, die Dokumentation und Sicherung der Flugdaten sowie weitere mechanische und elektronische Tests. Zudem sind ggf. Nutzlastdaten zu sichern.

GP2 enthält alle Wartungs- und Instandsetzungsarbeiten, die durchgeführt werden müssen, um die Betriebssicherheit aufrechtzuerhalten. GP2 beinhaltet alle Teilprozesse, die zwischen den Flügen des UAS durchzuführen sind, um die Betriebssicherheit zu erhalten. Dazu gehören die Prüfung und bei Bedarf Instandsetzung, der Austausch von informationsverarbeitenden Komponenten, die Aktualisierung der Flugbetriebssoftware, z.B. der Firmware oder Systemsoftware des zentralen Steuerrechners im UAS, sowie die Aktualisierung aller weiteren Softwarekomponenten nach Herstellervorgabe. Einige dieser Aufgaben sind nach bzw. vor jedem Flug durchzuführen, für andere gelten spezifische Vorgaben des Herstellers.

Zum Informationsverbund gehören neben den Geschäftsprozessen GP1 und GP2 weitere Anwendungen, mit denen die zu erledigenden Aufgaben unterstützt werden. Die nachfolgende Tabelle gibt einen Überblick über die typischen Anwendungen des Informationsverbundes.

Abkürzung	**Name der Software**
A01	Flugplanungssoftware
A02	Kartensoftware
A03	Wartungssoftware
A04	Flight-Control-Software
A05	Ground-Control-Software
A06	Flight-Data-Recorder[3]
A07	Payload-Steuerung
A08	Steuerung Zusatzaufgaben
A09	Configuration-Management-Software

Tabelle 2: Typische Anwendungen im Informationsverbund

[3] Der Flight Data Recorder ist eine technische Komponente der Drohne und stellt im Sinne des IT-Grundschutzprofils eine Größe dar, die nicht dem Einfluss der Anwender liegt. Die Maßnahmen für einen IT-Grundschutz liegen beim jeweiligen Hersteller der Drohne.

5.2.IT-Systeme

Im Informationsverbund sind neben den Geschäftsprozessen und Anwendungen auch die IT-Systeme zu betrachten.

Die nachfolgende Tabelle gibt eine Übersicht über die typischen IT-Systeme im Informationsverbund.

Abkürzung	**Name des IT-Systems**
C01	Desktoprechner
C02	Laptop
C03	Tablet oder Smartphone
S01	Server
D01	Flight-Controller
D02	Companion-Computer

Tabelle 3: Typische IT-Systeme im Informationsverbund

5.3.Netze und Netzkomponenten

Der Informationsverbund ist durch heterogene Netzwerke gekennzeichnet. Neben kabelgebundenen Netzen kommen Funknetze wie WLAN/IEEE 802.11 für die lokale Kommunikation, Mobilfunkstandards, IEEE 802.15.4 und spezifische Long-Range- und Satellitenkommunikationsverbindungen für die Kommunikation zwischen der Drohne in der Luft und der kontrollierenden Bodenstation zum Einsatz. Im Einzelnen sind dies in der Regel die Datenverbindung zwischen der Drohne und der Bodenkontrollstation (Telemetrie und Telecommand), Verbindungen zwischen der Drohne und anderen Luftfahrzeugen (ADS-B, OGN) und/oder Verbindungen zwischen der Bodenkontrollstation und anderen Luftverkehrsteilnehmern (USSP, ANSP etc.).

Die folgende Tabelle gibt einen Überblick über die typischen Netzwerkkomponenten im Informationsverbund.

Abkürzung	**Name der Netzwerkkomponente**
NET01	Aktive Komponenten kabelgebundenes Organisationsnetzwerk
NET02	Aktive Komponenten drahtloses Organisationsnetzwerk
NET03	Schnittstelle zwischen Organisations- und Datennetzwerk
NET04	On-board-Netzwerk der Drohne
NET05	Aktive Komponenten der Verbindung Drohne zu Bodenkontrollstation

Tabelle 4: Typische Netzwerkkomponenten im Informationsverbund

5.4.Infrastruktur: Räume und Gebäude

Komponenten des Informationsverbundes können in einem Gebäude, in einem Fahrzeug (dazu sogleich unter Kapitel 5.5), außerhalb von Gebäuden oder Fahrzeugen und in der Drohne untergebracht sein. Diese Infrastrukturbestandteile sind aus Sicht der Informationssicherheit ggf. unterschiedlich zu behandeln. Daher erfolgt hier und im nächsten Unterkapitel eine Differenzierung zwischen mobilen und stationären Infrastrukturobjekten.

Die nachfolgende Tabelle gibt einen Überblick über die typischen stationären Infrastrukturkomponenten im Informationsverbund.

Abkürzung	**Name des Raums oder Gebäudes**
R01	Allgemeiner Raum, zugangskontrolliert
R02	Leitstand/Bodenkontrollstation
R03	Halle, Werkstattbereich
R04	Labor
R05	Serverraum
R06	Außenbereich, zugangskontrolliert
R07	Flugtest- und Demonstrationsfläche
R08	Öffentlicher Raum

Tabelle 5: Typische Infrastrukturkomponenten im Informationsverbund

5.5.Infrastruktur: Fahrzeuge

Die UAS werden üblicherweise nicht am Sitz des UAS-Betreibers betrieben. Im Regelfall ist also der Transport von UAS zu berücksichtigen.

Die nachfolgende Tabelle gibt einen Überblick über die typischen mobilen Infrastruktur-komponenten im Informationsverbund.

Abkürzung	**Name der mobilen Infrastrukturkomponente**
F01	Transportfahrzeug für UA bzw. UAS
F02	Operation Vehicle
UA01	Unmanned Aircraft/Drohne

Tabelle 6: Typische mobile Infrastrukturkomponenten im Informationsverbund

In vielen Fällen sind F01 und F02 identisch, d.h. Transport und Betriebsunterstützung erfolgen in einem Fahrzeug.

5.6.Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der in diesem Kapitel dargestellten Referenzarchitektur ab, so sind die zusätzlich vorhandenen Zielobjekte im Rahmen der

Strukturanalyse zu dokumentieren. Diesen Zielobjekten müssen passende Komponenten des IT-Grundschutz-Kompendiums zugeordnet werden.

Zielobjekte aus diesem IT-Grundschutz-Profil, die im zu schützenden Informationsverbund nicht vorkommen, brauchen entsprechend nicht berücksichtigt zu werden.

5.7. Komponenten in Beziehung zu den Zielobjekten im Informations-verbund

Die folgende Tabelle ordnet die Komponenten den Zielobjekten im Informationsverbund zu.

Diese Beziehung stellt den Rahmen für die Auswahl der relevanten Bausteine für die jeweilige Organisation dar, die das IT-Grundschutz-Profil anwendet.

Komponente	Anzuwenden auf Zielobjekt
A01 Flugplanungssoftware	GP1
A02 Kartensoftware	GP1
A03 Wartungssoftware	GP2
A04 Flight-Control-Software	GP1
A05 Ground-Control-Software	GP1
A06 Flight-Data-Recorder	GP1
A07 Payload-Steuerung	GP1
A08 Steuerung Zusatzaufgaben	GP1
A09 Configuration-Management-Software	GP2
C01 Desktoprechner	A01, A03, A05, A07, A08, A09
C02 Laptop	A01, A03, A05, A07, A08, A09
C03 Tablet	A01, A03, A05, A07, A08, A09
S01 Server	A02
D01 Flight-Controller	A04
D02 Companion-Computer	A07, A08
NET01 Kabelgebundenes Netzwerk	C01, C02, S01
NET02 Drahtloses Netzwerk	C01, C02, C03
NET03 Schnittstellen Nw/Datennw.	C01, C02, C03, S01, D01, D02
NET04 On-board-Netzwerk	D01, D02
NET05 Drohne Bodenkontrollstation	C01, C02, C03, D01, D02
R01 Allgemeiner Raum, zugangskontrolliert	C01, C02, C03, NET01, NET03
R02 Leitstand/Bodenkontrollstation	C01, C02, C03
R03 Halle, Werkstattbereich	C01, C02, C03, D01, D02
R04 Labor	C01, C02, C03, D01, D02
R05 Serverraum	S01
R06 Außenbereich, zugangskontrolliert	C02, C03, D01, D02
R07 Flugtest- und Demonstrationsfläche	C02, C03, D01, D02
R08 Öffentlicher Raum	C02, C03, D01, D02
F01 Transportfahrzeug	D01, D02
F02 Operation Vehicle	C01, C02, C03, S01
UA01 Unmanned Aircraft	D01, D02

Tabelle 7: Anzuwendende Bausteine

6. Feststellung des Schutzbedarfs

Für die im Rahmen der Strukturanalyse ermittelten Prozesse, Anwendungen, IT- und Kommunikationssysteme sowie Infrastrukturkomponenten ist zunächst der Schutzbedarf festzulegen. Grundlage dafür sind die Auswirkungen, die Verletzungen der Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) hätten. Geeignete Ansprechpartner für die Schutzbedarfsfeststellung sind beispielsweise die jeweiligen Prozess-verantwortlichen oder der Dateneigentümer der im jeweiligen Prozess verarbeiteten Daten. Der Schutzbedarf richtet sich grundsätzlich nach dem Umfang aller Daten, die in den Prozessen verarbeitet werden. Die Vorgehensweise bei der Feststellung des Schutzbedarfes ist im BSI-Standard 200-2 (siehe Kapitel 8.2) im Detail beschrieben. Der BSI-Grundschutz benennt verschiedene Szenarien, auf die sich ein Schaden beziehen kann. Diese sind in der folgenden Tabelle aufgeführt:

Identifikator	**Schadensszenario**
SZ1	Verstöße gegen Gesetze, Vorschriften oder Verträge
SZ2	Beeinträchtigungen des informellen Selbstbestimmungsrechts
SZ3	Beeinträchtigungen der persönlichen Unversehrtheit
SZ4	Beeinträchtigungen der Aufgabenerfüllung
SZ5	Negative Innen- oder Außenwirkung
SZ6	Finanzielle Auswirkungen

Tabelle 8: Potenzielle Schadensszenarien

Die konkreten Auswirkungen und möglichen Schadensszenarien können je nach Anwendungsfall variieren. In der nachfolgenden Tabelle sind mögliche Beispiele zu den Schadens-szenarien aufgeführt:

Identifikator	Beispiele für Schadensszenarien
SZ1	Veränderte oder unvollständige Daten können zu Verstößen gegen Gesetze und Vorschriften (beispielsweise Flug innerhalb eines nicht erlaubten Fluggebiets) oder zu Verstößen gegen Verträge mit Geschäftspartner/innen (beispielsweise Videoaufzeichnung nicht im vereinbarten Fluggebiet) führen.
SZ2	Personenbezogene Daten von Mitarbeiter/innen oder Geschäftspartner/innen oder sensible Unternehmensdaten werden ohne Autorisierung öffentlich oder unbefugten Dritten zugänglich. Unternehmenskritische bzw. -vertrauliche Daten werden ohne Autorisierung öffentlich oder unbefugten Dritten zugänglich. Dies kann zu finanziellen Nachteilen führen.
SZ3	Eine unvollständige oder fehlerhafte Datenübertragung oder die Übertragung schädlich veränderter Daten führt zur Fehlsteuerung des UAS, zu falschen Entscheidungen im Prozessablauf (Flugbetrieb oder Wartung/Instandsetzung) und in der Folge zu Unfällen mit Personenschäden.
SZ4	Eine unvollständige oder schädlich veränderte Datenübertragung führt zu einem Abbruch des Flugbetriebs (GP1), der Videoaufzeichnung (GP1) oder zu einer fehlerhaften Wartung bzw. Instandsetzung des UAS (GP2) und damit zu einer eingeschränkten oder ausgefallenen Aufgabenerfüllung. Ein nicht- oder nur eingeschränkt verfügbares Teil des Informationsverbundes führt zu einem Abbruch des Flugbetriebs oder zu einer Beendigung der Videoaufzeichnung und damit zu einer eingeschränkten Aufgabenerfüllung.
SZ5	Ein eingeschränkter oder abgebrochener Flugbetrieb (GP1) bzw. eine unvollständige Videoaufzeichnung (GP1) führen zu Imageschäden und Vertrauensverlust. Eine unvollständige oder fehlerhafte Wartung und Instandsetzung führt zu Imageschäden und Vertrauensverlust.
SZ6	Ein unvollständiger Flugbetrieb (GP1) bzw. eine unvollständige Videoaufzeichnung (GP1) führt zu Dienstleistungs- oder Prozessausfällen bzw. Kosten für die erneute Durchführung des Prozesses. Ein fehlerhafter Flugbetrieb mit Schadensfolge führt zu zusätzlichen Kosten. Eine fehlerhafte oder unvollständige Wartung und Instandsetzung führen zu zusätzlichen Material- und Personalkosten.

Tabelle 9: Beispiele von Schadensszenarien

Die Auswirkung eines Schadens ist im Voraus nicht bestimmbar. Daher empfiehlt die Methodik des IT-Grundschutzes des BSI die Klassifizierung in die drei Kategorien normal, hoch und sehr hoch im Zusammenhang mit der Schutzbedarfsermittlung. In der folgenden Tabelle sind die Kategorien, ergänzt um die generischen Schadensauswirkungen, aufgeführt. Die Auswirkungen können sich auf Komponenten, das Unternehmen oder betroffene Dritte beziehen:

Kategorie	Schadensauswirkung
normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein.
sehr hoch	Die Schadensauswirkungen können ein existenz- oder lebensbedrohliches Ausmaß erreichen.

Tabelle 10: Beispiele des BS für Schutzbedarfskategorien

Werden in einem Schadensszenario beträchtliche, existenzbedrohende oder lebensbedrohliche Auswirkungen festgestellt, so ist der betroffene Grundwert im Schutzbedarf mit hoch oder sehr hoch einzustufen, in allen anderen Fällen mit normal. Im Weiteren wird der ermittelte Schutzbedarf je Grundwert auf die Schicht der Anwendungen vererbt, anschließend in weiteren Schritten auf die IT-Systeme, auf die Netze, die Räumlichkeiten und Infrastrukturobjekte.

Eine konkrete Schutzbedarfsfeststellung muss auf der Grundlage des IT-Grundschutzprofils im Einzelfall durch den Anwender erfolgen.

6.1. Risikobetrachtung

Auch bei Umsetzung aller Anforderungen ist keine hundertprozentige Sicherheit zu erreichen. Dies muss sowohl den Anwendern des IT-Grundschutz-Profils als auch den Entscheidungsträgern bewusst sein. Aufgrund der Besonderheiten beim Flugbetrieb mit Drohnen ist in jedem Fall eine Risikoanalyse zu erstellen.

Insbesondere für die Zielobjekte UAS/Drohne und ggf. der Bodenkontrollstation gibt es im IT-Grundschutz-Kompendium keine passenden Bausteine, sodass bis auf Weiteres eine Risikoanalyse zwingend erforderlich ist. Es wird das Vorgehen der Risikoanalyse nach dem BSI-Standard 200-3 empfohlen. In diesem BSI-Standard werden bereits 47 elementare Gefährdungen aufgeführt, die im IT-Grundschutz-Kompendium näher erläutert werden. Diese Gefährdungen sollten dabei Ausgangspunkt für die Erstellung der Gefährdungsübersicht sein und sollten bei Bedarf jedoch ergänzt werden.

Im Rahmen der Risikoanalyse werden folgende Schritte durchlaufen:

- eine Gefährdungsübersicht erstellen,
- eine Risikoeinschätzung vornehmen,
- die Risikobehandlung festlegen,
- Konsolidierung der erweiterten Sicherheitsmaßnahmen mit den Ergebnissen des IT-Grundschutz-Checks.

Somit wird sichergestellt, dass im Rahmen der Risikoanalyse definierte höherwertige Sicherheitsmaßnahmen auch auf Objekte mit normalen Schutzbedarf Anwendung finden, sofern dies sinnvoll ist. Dabei ist zu berücksichtigen, dass Aspekte der Flugsicherheit im Rahmen des Flugsicherheitsmanagements separat betrachtet werden. Sie sind daher nicht Bestandteil dieses IT-Grundschutz-Profils.

6.2. Vorbereitung der Risikoanalyse

Als Grundlage für die Vorbereitung der Risikoanalyse und die Ermittlung des Gefährdungspotentials der Anwendungen, für die dieses IT-Grundschutz-Profil angewendet wird, dient die zu diesem Profil zugehörige Tabelle. Gefährdungsmatrix. Die Tabelle kann als zusätzliche Datei über die Webseite des BSI, gleich neben diesem Profil, bezogen werden.

7. Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschutz-Kompendium des BSI stellt Prozess- und Systembausteine bereit, die anwendungsbezogene Anforderungen zur Umsetzung des IT-Grundschutzes vorgeben.

7.1. Auswahl der Prozessbausteine

Auf jeden Informationsverbund sind die übergreifenden Prozess-Bausteine anzuwenden. Diese behandeln Sicherheitsaspekte, die für große Teile des Informationsverbundes gleichermaßen gelten.

ISMS: Sicherheitsmanagement

ID	Baustein	relevant	Begründung (falls nicht relevant)
ISMS.1	Sicherheitsmanagement	ja	

Tabelle 11: ISMS-Schicht

ORP: Organisation und Personal

ID	Baustein	relevant	Begründung (falls nicht relevant)
ORP.1	Organisation	ja	
ORP.2	Personal	ja	
ORP.3	Sensibilisierung und Schulung zur Informationssicherheit	ja	
ORP.4	Identitäts- und Berechtigungsmanagement	ja	
ORP.5	Compliance Management	ja	

Tabelle 12: ORP-Schicht

CON: Konzeption und Vorgehensweise

ID	Baustein	relevant	Begründung (falls nicht relevant)
CON.1	Kryptokonzept	ja	Im Rahmen der Beschaffung von Drohnen durch CE Verfahren definiert. Unterliegt nicht dem Einfluss des Anwenders.
CON.2	Datenschutz	ja	
CON.3	Datensicherungskonzept	ja	
CON.4	(entfallen)		(intentionally left blank)
CON.5	(entfallen)		(intentionally left blank)
CON.6	Löschen und Vernichten	ja	Durch Hersteller im Rahmen CE Verfahren definiert. Unterliegt nicht dem Einfluss des Anwenders.
CON.7	Informationssicherheit auf Auslandsreisen	nein	Nicht im Betrachtungsbereich; konzeptionell irrelevant
CON.8	Software-Entwicklung	nein	Keine Software-Entwicklung im Informationsverbund
CON.9	Informationsaustausch	ja	
CON.10	Entwicklung von Webanwendungen	nein	Keine Entwicklung von Webanwendungen im Informationsverbund

Tabelle 13: CON-Schicht

OPS: Betrieb

ID	Baustein	relevant	Begründung (falls nicht relevant)
OPS.1.1.1	Allgemeiner IT-Betrieb	ja	Erfüllung der Basisanforderungen, d.h. Festlegung von Rollen und Berechtigungen sowie Festlegung von Aufgaben und Zuständigkeiten, im Übrigen abhängig von Relevanz für den Drohnen-Betrieb
OPS.1.1.2	Ordnungsgemäße IT-Administration	ja	
OPS.1.1.3	Patch- und Änderungsmanagement	ja	
OPS.1.1.4	Schutz vor Schadprogrammen	ja	
OPS.1.1.5	Protokollierung	ja	
OPS.1.1.6	Software-Tests und Freigaben	ja	Eingeschränkt gem. Herstellervorgaben
OPS.1.1.7	Systemmanagement	ja	
OPS.1.2.1			(intentionally left blank)
OPS.1.2.2	Archivierung	ja	
OPS.1.2.3			(intentionally left blank)
OPS.1.2.4	Telearbeit	nein	nicht anwendbar
OPS.1.2.5	Fernwartung	ja	Eingeschränkt gem. Herstellerangaben
OPS.1.2.6	NTP-Zeitsynchronisation	ja	
OPS.2.1	Outsourcing für Kunden	nein	Hier nicht betrachtet, konzeptionell irrelevant
OPS2.2	Cloud-Nutzung	ja	(je nach Konfiguration)
OPS3.1	Outsourcing für Dienstleister	ja	(je nach Anwendungsszenario)

Tabelle 14: OPS-Schicht

DER: Detektion und Reaktion

ID	Baustein	relevant	Begründung (falls nicht relevant)
DER.1	Detektion von sicherheitsrelevanten Ereignissen	ja	
DER.2.1	Behandlung von Sicherheitsvorfällen	ja	
DER.2.2	Vorsorge für die IT-Forensik	ja	Flugsicherheit/Flugunfalluntersuchung
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	ja	
DER.3.1	Audits und Revisionen	ja	Empfehlung: kontinuierlicher Verbesserungsprozess beim Drohnen-Anwender implementieren
DER.3.2	Revision auf Basis des Leitfadens IS-Revision	nein	Nur für Bundesbehörden vorgeschrieben
DER.4	Notfallmanagement	ja	In Verbindung mit Hersteller

Tabelle 15: DER-Schicht

7.2. Auswahl der System-Bausteine

In den folgenden Tabellen werden die System-Bausteine aufgeführt. Hier ist entscheidend, ob der jeweilige Baustein für eine spezifische Komponente des hier betrachteten Informationsverbunds relevant ist. Es wird darauf hingewiesen, dass System-Bausteine der Schicht INF in der Offenen Kategorie (UAS Open) in der Regel nicht Bestandteil des Informationsverbundes dieses IT-Grundschutz-Profils sind.

APP: Anwendungen

ID	Baustein	Zielobjekte	relevant	ggf. Begründung
APP.1.1	Office-Produkte		nein	nicht Teil des Informationsverbundes
APP.1.2	Web-Browser	C01, C02, C03, S01	ja (ggf.)	
APP.1.4	Mobile Anwendungen		ja (ggf.)	
APP.2.1	Allg. Verzeichnisdienst		ja (ggf.)	
APP.3.1	Webanwendungen		ja (ggf.)	
APP.3.2	Webserver		ja	
APP.3.3	Fileserver	C01, C02, C03	ja	
APP.3.4	DNS-Server		nein	nicht Teil des Informationsverbundes
APP.4.2	SAP-ERP-System		nein	nicht Teil des Informationsverbundes
APP.4.3	Relationale Datenbanksysteme		nein	nicht Teil des Informationsverbundes
APP.4.6	SAP-ABAP-Programmierung		nein	nicht Teil des Informationsverbundes
APP.5.2	Microsoft Exchange und Outlook		nein	nicht Teil des Informationsverbundes
APP.5.3	Allgemeiner E-Mail-Client und –Server		nein	nicht Teil des Informationsverbundes
APP.6	Allgemeine Software		ja	
APP.7	Entwicklung von Individualsoftware		nein	Es findet keine Entwicklung von Software im Informationsverbund statt.

Tabelle 16: APP-Schicht

SYS: IT-Systeme

ID	Baustein	Zielobjekte	relevant	ggf. Begründung
SYS.1.1	Allgemeine Server	S01	ja	
SYS.2.1	Allgemeiner Client	C01	ja	
SYS.3.1	Laptops	C02, C03	ja	
SYS.4.3	Eingebettete Systeme	D01, D02	ja	
SYS.4.4	Allgemeines IoT-Gerät			

Tabelle 17: SYS-Bausteine

Die Bausteine **der Schichten IND: Industrielle IT, NET: Netze und Kommunikation und INF: Infrastruktur** werden aktuell in diesem Profil nicht betrachtet. Sie müssen von den Anwendenden im Rahmen des Sicherheitsprozesses individuell betrachtet und modelliert werden.

7.3.Zugangskontrollen

Daten unterliegen u. U. Regularien, so dass man gewährleisten muss, dass der Zugriff entsprechend limitiert ist und dokumentierbar sein muss. Gleichzeitig sollte eine leichte Pflege ermöglicht werden. Die hier oft umgesetzten Modelle sind IBAC, RBAC und ABAC oder hybride Varianten dieser 3 Modelle.

8. Restrisikobetrachtung

Der Flugbetrieb mit unbemannten Luftfahrzeugen der offenen Kategorie erfordert derzeit bei Einhaltung der Grundsätze dieses IT-Grundschutz-Profils keine allgemeine Restrisikobetrachtung.

9. Anwendungshinweise

Die ermittelten Anforderungen sind in das Gesamtsicherheitskonzept zu integrieren und umzusetzen. Dazu hat sich der PDCA-Zyklus (Plan, Do, Check, Act) bewährt, d.h. ein sich wiederholender Prozess der Planung, Umsetzung, Überprüfung und Anpassung, um kontinuierlich das gewünschte Sicherheitsniveau aufrecht erhalten zu können.

10. Unterstützende Informationen

Detailliertere Informationen zu den einzelnen Anforderungen finden sich in den Umsetzungshinweisen der einzelnen Bausteine des IT-Grundschutzes.

Spezielle Informationen zur Umsetzung der Anforderungen des § 13 TMG finden sich in der BSI-Publikation "Absicherung von Telemediendiensten nach Stand der Technik".

Darüber hinaus gelten die einschlägigen nationalen und internationalen Vorschriften und Regelungen für den Flugbetrieb mit unbemannten Luftfahrzeugen.

Anlage 1 – Bausteine/Systemkomponenten

Abkürzung	Bezeichnung
A01	Flugplanungssoftware
A02	Karten-Software
A03	Wartungssoftware
A04	Flight Control-Software
A05	Ground Control-Software
A06	Logbuch/Flight Data Recorder
A07	Payload-Steuerung
A08	Steuerung Zusatzaufgaben
A09	Configuration Management-Software
C01	Desktoprechner
C02	Laptop
C03	Tablet
S01	Server
D01	Flightcontroller des UA
D02	Companion-Computer
NET01	Aktive Komponenten kabelgebundenes Firmennetzwerk
NET02	Aktive Komponenten drahtloses Firmennetzwerk
NET03	Schnittstelle zwischen Firmen- und Datennetzwerk
NET04	OnBoard-Netzwerk des UA
R01	Zugangskontrollierter Raum (Die Zugangskontrollen sind spezifisch für die Institution und die Gefährdungslage und sind individuell anzupassen. Im Idealfall sind alle Räume und Flächen zugangskontrolliert.)
R02	Leitstand (Bodenkontrollstation)
R03	Halle, Werkstattbereich
R04	Labor
R05	Serverraum
R06	Außenbereich, zugangskontrolliert[1]
R07	Flugtest- und Demonstrationsfläche
R08	Öffentlicher Raum
F01	Transportfahrzeug für UA bzw. UAS
F02	Operation Vehicle
UA01	Unmanned Aircraft/Drohne

Tabelle 18: Bausteine/Systemkomponenten

Anlage 2 – Elementare Gefährdungen

Abkürzung	Bezeichnung
G 0.1	Feuer
G 0.2	Ungünstige klimatische Bedingungen
G 0.3	Wasser
G 0.4	Verschmutzung Staub Korrosion
G 0.5	Naturkatastrophen
G 0.6	Katastrophen im Umfeld
G 0.7	Großereignisse im Umfeld
G 0.8	Ausfall oder Störung der Stromversorgung
G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.10	Ausfall oder Störung von Versorgungsnetzen
G 0.11	Ausfall oder Störung von Dienstleistern
G 0.12	Elektromagnetische Störstrahlung
G 0.13	Abfangen kompromittierender Strahlung
G 0.14	Ausspähen von Informationen (Spionage)
G 0.15	Abhören
G 0.16	Diebstahl von Geräten Datenträgern oder Dokumenten
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- und Software
G 0.22	Manipulation von Informationen
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.24	Zerstörung von Geräten oder Datenträgern
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.27	Ressourcenmangel
G 0.28	Software-Schwachstellen oder -Fehler
G 0.29	Verstoß gegen Gesetze oder Regelungen
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32	Missbrauch von Berechtigungen

G 0.33	Personalausfall
G 0.34	Anschlag
G 0.35	Nötigung, Erpressung oder Korruption
G 0.36	Identitätsdiebstahl
G 0.37	Abstreiten von Handlungen
G 0.38	Missbrauch personenbezogener Daten
G 0.39	Schadprogramme
G 0.40	Verhinderung von Diensten (Denial of Service)
G 0.41	Sabotage
G 0.42	Social Engineering
G 0.43	Einspielen von Nachrichten
G 0.44	Unbefugtes Eindringen in Räumlichkeiten
G 0.45	Datenverlust
G 0.46	Integritätsverlust schützenswerter Informationen
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe

Tabelle 19: Elementare Gefährdungen

Anlage 3 – Begriffsdefinitionen

Begriff	Definition
Informationssicherheit	Umfassende Bezeichnung für alle Elemente im Zusammenhang mit der Erfassung, Nutzung und Speicherung von Daten einschließlich Informationstechnik.
Grundschutz	Zustand, der durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen ein Sicherheitsniveau erreicht, das für den jeweiligen Schutzbedarf angemessen und ausreichend ist, um institutionsrelevante Informationen zu schützen. BSI – IT-Grundschutzkompendium Kapitel 1.2).
Erhöhter Schutzbedarf	Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Dabei können szenarienbedingte Besonderheiten auftreten, die unabhängig von der Schutzbedarfskategorie eine spezifische Risikoanalyse erfordern und ggf. punktuelle oder zeitliche Maßnahmen bewirken.
Risikoanalyse	Bezeichnung des kompletten Prozesses, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. (BSI – IT-Grundschutzkompendium Glossar).
Organisationsnetzwerk	Das IT- und Kommunikationsnetzwerk des jeweiligen Luftfahrtbetriebs.
Datennetzwerk	Digitale Ablagedienste außerhalb des Organisationsnetzwerks, ugs.: Cloud.
Unmanned Aircraft Systems	In diesem IT-Grundschutz-Profil wird einheitlich der international standardisierte Oberbegriff verwendet. Er umfasst alle Systembezeichnungen und Unterkategorien, die unbemannte Luftsysteme bezeichnen, wie z.B. Drohne, Remotely Piloted Aircraft System (RPAS) etc. In diesem Zusammenhang bezeichnet der Begriff Unmanned Aircraft (UA) das fliegende Element des Systems. Der Begriff Unmanned Aerial Vehicle (UAV) ist veraltet und sollte nicht mehr verwendet werden.

Tabelle 20: Begriffsdefinitionen

Anlage 4 – Abkürzungen

Abkürzung	Begriff
ABAC	Attribute Based Access Control
ADS-B	Automatic Dependent Surveillance - Broadcast
ANSP	Air Navigation Service Provider
BDSG	Bundesdatenschutzgesetz
DNS	Domain Name System
DSGVO	Datenschutzgrundverordnung
GP	Geschäftsprozess
IBAC	Identity Based Access Control
IT	Informationstechnik
JARUS	Joint Authorities for Rulemaking on Unmanned aircraft Systems
OGN	Open Glider Network
RBAC	Role Based Access Control
SAP ABAP	Advanced Business Application Programming (SAP-Produkt)
SAP ERP	Enterprise Resource Planning (SAP-Produkt)
TMG	Telemediengesetz
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
UAS	Unmanned Aircraft System
USSP	U-Space Service Provider

Tabelle 21: Abkürzungen