

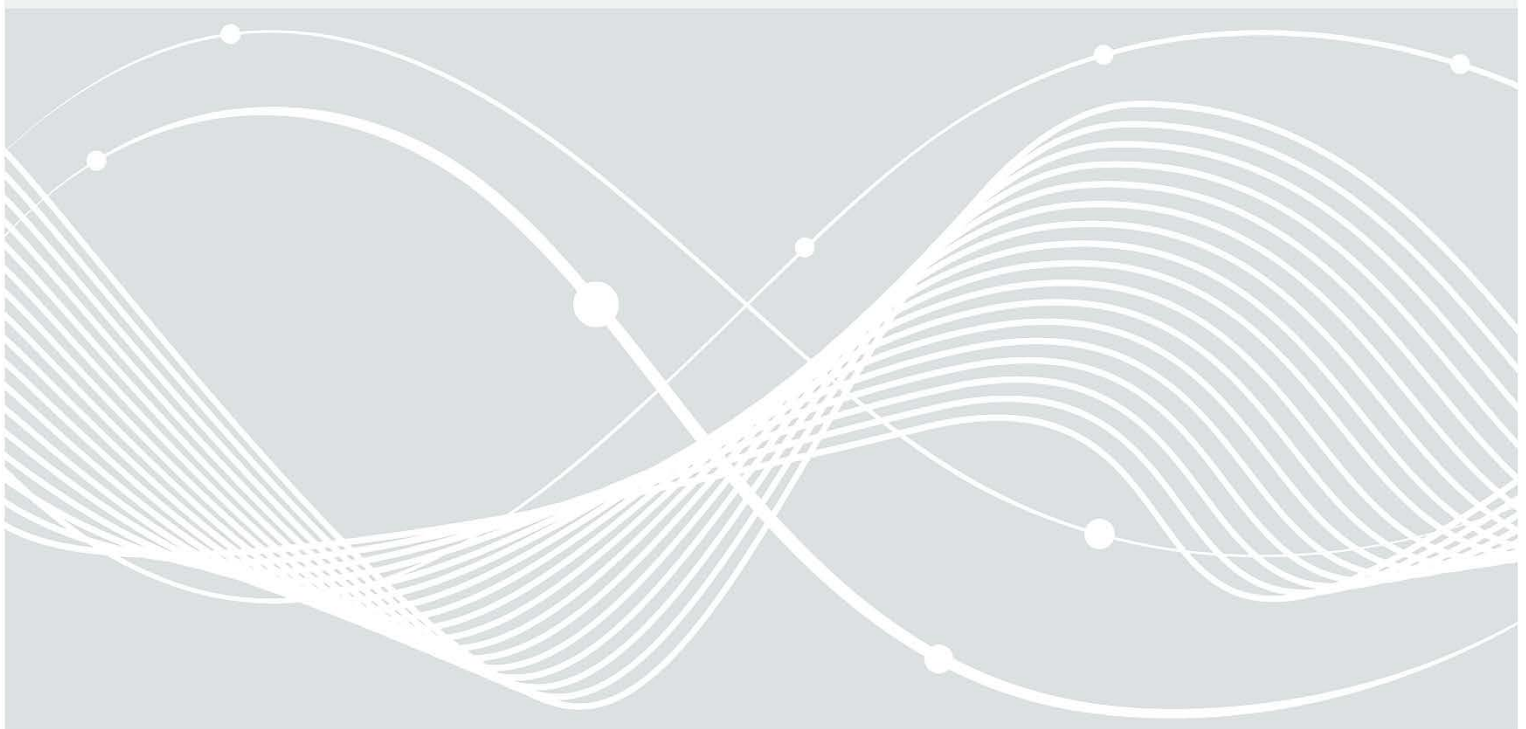


Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

IT-Grundschutz-Profil für Weltrauminfrastrukturen

Mindestabsicherung für den Satelliten über den gesamten Lebenszyklus



Änderungshistorie

Tabelle 1: Änderungshistorie

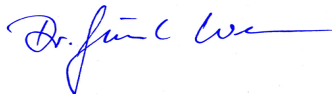
<i>Version</i>	<i>Datum</i>	<i>Name</i>	<i>Beschreibung</i>
1.0	30.06.2022		Erstveröffentlichung

Vorwort des Abteilungsleiters Krypto-Technik und IT-Management

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2021 eine Arbeitsgruppe, bestehend aus Experten des BSI, OHB Digital Connect und Airbus Defence and Space sowie der Deutschen Raumfahrtagentur im Deutschen Zentrum für Luft- und Raumfahrt (DLR) initiiert, um gemeinsam Mindestanforderungen an die Cybersicherheit für Satelliten zu erstellen. Damit setzt das BSI erste Maßnahmen um, welche zur Erreichung der in der *BSI-Strategie für Cybersicherheit im Weltraum* definierten Handlungsziele identifiziert wurden. Letztere leiten sich aus dem Leitziel der Strategie ab, der *Stärkung der Cybersicherheit von Weltrauminfrastrukturen, welche von Relevanz für Staat, Wirtschaft und Gesellschaft sind, zur Sicherstellung der Verfügbarkeit von Diensten über integrale, authentische Kommunikation*.

Zum Zwecke der Erstellung gemeinsamer Mindestanforderungen veranstaltete das BSI eine Workshop-Reihe, aus der in einem ersten Schritt das vorliegende branchenspezifische IT-Grundschutz-Profil hervorging. Es beinhaltet Empfehlungen für eine Mindestabsicherung aller Satellitenmissionen. Das Profil soll eine Empfehlung und Handreichung sein, welche Raumfahrtakteuren eine wirkungsvolle Umsetzung eines Sicherheitskonzepts ermöglichen. Wenngleich unternehmens- und missionsspezifische Anpassungen nötig sein können, dient dieses Profil aufgrund der im Grundsatz relativ ähnlichen Prozesse, angelehnt an die Lebensphasen eines Satelliten, als Schablone, den individuell passenden Schutzbedarf zu bestimmen und umzusetzen. Um ferner auf die sehr unterschiedlichen Schutzbedarfe bei verschiedenen Satellitenmissionen eingehen zu können, ist es vorgesehen, die Anforderungen nach Erstellung des Grundschutz-Profiles in verschiedenen Technischen Richtlinien zu detaillieren und im internationalen Kontext zu etablieren.

Ich danke den Mitgliedern der Arbeitsgruppe für Ihre Bereitschaft, bei der Erstellung des vorliegenden IT-Grundschutz-Profiles mitzuwirken.



Dr. Günther Welsch

Leiter Abteilung Kryptotechnik und IT-Management

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik, OHB Digital Connect GmbH, Airbus CyberSecurity GmbH, Raumfahrtagentur des Deutschen Zentrums für Luft- und Raumfahrt

Version: 1.0

Revisionszyklus: 2-jährlich

Version IT-Grundschutz-Kompendium 2022

Abkürzungsverzeichnis

Tabelle 2: Abkürzungsverzeichnis

Abkürzung	Bedeutung
AIT	Assembly, Integration and Test
AIV	Assembly, Integration and Verification
ASW	Application Software
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCPA	California Consumer Privacy Act
CCSDS	Consultative Committee for Space Data Systems
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DMS	Dokumentenmanagementsystem
DNS	Domain Name System
DPA	Data Processing Agreement
ECSS	<i>European Cooperation for Space Standardization</i>
EGSE	Electrical Ground Support Equipment
ERP	Enterprise Resource Planning
FPGA	Field Programmable Gate Array
GEO	Geostationary Earth Orbit
GDPR	General Data Protection Bill
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IC	Integrated Circuit
IDE	Integrated Design Engineering
IDS	Integrated Detection System
IoT	Internet of Things
IPS	Integrated Prevention System
ISMS	Information Security Management System
KRITIS-V	KRITIS Verordnung
LDAP	Lightweight Directory Access Protocol
LEO	Low Earth Orbit
MDM	Mobile Device Management
MEO	Medium Earth Orbit
MGSE	Mechanical Ground Support Equipment
NIST	National Institute of Standards and Technology
OBC	On Board Computer
OTRS	Open Ticket Request System
PDPB	Personal Data Protection Bill
PL	Payload
Requirement-Eng/Mgt	Requirement Engineering and Management System
RT-OS	Real Time Operating System
SatDSiG	Satellitendatensicherheitsgesetz
SCM	Supply Chain Management
SQL	Structured Query Language
STK	Systems Tool Kit
TK	Telekommunikation

Inhalt

1	Einleitung	8
1	Formale Aspekte.....	9
2	Haftungsausschluss.....	9
3	Liste der Autorinnen und Autoren.....	9
4	Management Summary	10
4.1	Zielgruppe	10
4.2	Zielsetzung.....	10
4.3	Aufgaben der Leitungsebene.....	11
5	Festlegung des Geltungsbereichs	11
5.1	Zielgruppe	11
5.2	Beschreibung des Schutzbedarfs	12
5.3	IT-Grundschutz Vorgehensweise.....	12
5.4	Kompatibilität zu anderen Standards	12
5.5	Berücksichtigte Rahmenbedingungen	12
6	Abgrenzung des Informationsverbundes.....	13
6.1	Bestandteile des Informationsverbundes.....	13
6.2	Nicht berücksichtigte Teile	13
7	Referenzarchitektur.....	13
7.1	Prozesse	13
7.2	Anwendungen	14
7.3	IT-Systeme	16
7.4	Netze und Netzkomponenten	18
7.4.1.	Netzplan.....	19
7.5	Gebäude und Räume	20
7.6	Annahmen und Erläuterungen.....	20
7.7	Umgang mit Abweichungen.....	23
8	Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	23
8.1	Feststellung des Schutzbedarfs.....	23
8.1.1.	Rahmenbedingungen	23
8.1.2.	Methodik	23
8.1.3.	Beispielmissionen.....	24
8.1.4.	Schutzbedarf, Regulatorik und Szenarien.....	24
8.1.5.	Ergebnis der generischen Schutzbedarfsanalyse.....	26
8.1.6.	Hinweise zur Erstellung einer individuellen Schutzbedarfsfeststellung	26
8.2	Auswahl relevanter Bausteinen	27
8.2.1.	Übergreifende Bausteine (gesamter Informationsverbund).....	27

8.2.2.	Bausteine pro Zielobjekt.....	29
8.3	Anforderungen an Satelliten	32
8.3.1.	Allgemeine Anforderungen.....	32
8.3.2.	Anforderungen an den Transport.....	33
8.3.3.	Starteinrichtung.....	33
8.3.4.	Schnittmenge In Orbit Phase und Bodensegment	33
8.3.5.	Außerbetriebnahme	34
9	Restrisiko	35
10	Anwendungshinweise.....	35
11	Checkliste – Mindestanforderungen für die IT-Sicherheit in Weltrauminfrastrukturen.....	36

1 Einleitung

Eine Absicherung der Satelliten durch technische und organisatorische Maßnahmen empfiehlt sich für jede Satellitenmission. Nur für einige Missionen ist eine Absicherung für Teilaspekte verpflichtend. Missionen, die unter die KRITIS-Verordnung fallen, sind nach dem aktuellen Stand der Technik abzusichern, dies betrifft derzeit jedoch nur das europäische Satellitennavigationssystem GALILEO und dabei auch lediglich die Bodeninfrastruktur. Es existieren derzeit keine Regularien, die eine Umsetzung der Informationssicherheit beim Satelliten selbst bei dessen Herstellung (insb. unter Berücksichtigung des Security-by-Design-Konzeptes) und im Betrieb fordern und steuern. Somit liegt die Realisierung einer Absicherung durch die Unternehmen in deren Eigenverantwortung bzw. in den Vorgaben des Kunden. Das vorliegende Dokument „IT-Grundschutz-Profil für Weltrauminfrastrukturen – Mindestabsicherung für den Satelliten“ soll dabei durch die Formulierung von Anforderungen für eine *Mindestabsicherung* bei der Herstellung und dem Betrieb von Satelliten eine Hilfestellung geben.

Der Schutzbedarf der unterschiedlichen Satellitenmissionen erstreckt sich über die Kategorien „Normal“ bis „Sehr hoch“. Um möglichst alle Satellitenmissionen zumindest grundlegend abdecken zu können, wurde die Schutzbedarfskategorie „Normal“ zugrunde gelegt und eine entsprechende Absicherung entwickelt. Durch diese Maßnahmen zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität sollen hohe materielle und immaterielle Schäden über alle Lebensphasen eines Satelliten hinweg minimiert werden. Die zur Erfüllung der Schutzziele beschriebenen Maßnahmen müssen auf jede Mission individuell angepasst und je nach Kritikalität ggf. noch erweitert bzw. ergänzt werden.

In enger Zusammenarbeit haben das Bundesamt für Sicherheit in der Informationstechnik (BSI), OHB Digital Connect, Airbus und die Deutsche Raumfahrtagentur im Deutschen Zentrum für Luft- und Raumfahrt (DLR) dieses Profil entwickelt, mit dem Ziel, Empfehlungen für die Umsetzung der Informationssicherheit für Hersteller, Betreiber sowie Zulieferer von Satelliten bzw. ihrer Komponenten zu erstellen.

Ein IT-Grundschutz-Profil dient als Leitlinie zum strukturierten Erstellen eines IT-Sicherheitsprozesses. Es ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit vergleichbaren Rahmenbedingungen dienen soll. Schritte, die nach dem IT-Grundschutz zu gehen sind, sind in diesem Muster pauschalisiert, sodass es schließlich allen interessierten Satellitenherstellern und -betreibern möglich sein sollte, mit Hilfe der Schablone die Informationssicherheit zu erhöhen.

Ausgehend von sechs als relevant betrachteten Geschäftsprozessen, die an den Lebenszyklus eines Satelliten angelehnt und in Kapitel 7.1 definiert sind, umfasst das vorliegende Grundschutz-Profil

- eine Liste der relevanten Zielobjekte (Anwendungen, IT-Systeme sowie Räumlichkeiten), die es zu schützen gilt,
- eine Zuordnung der dazu passenden IT-Grundschutz-Bausteine mit Anforderungen und Umsetzungshinweisen, sowie
- Anforderungen, die aufgrund ihrer typischen Satellitenspezifika über den Grundschutz hinausgehen. Hierzu wird eine Checkliste bereitgestellt, die bei der Implementierung der für die jeweilige Mission als notwendig erachteten Sicherheitsanforderungen unterstützen kann. Diese Checkliste erfüllt keinen Anspruch auf Vollständigkeit und kann missionspezifisch angepasst werden.

Das IT-Grundschutz-Profil ist kompatibel zu dem Anforderungskatalog der Deutschen Raumfahrtagentur im DLR (Tailoring Catalogue – Product Assurance, Safety & Sustainability Requirements for DLR Space Projects, DLR-RF-PS-001), welches die IT-Grundschutz-Methodik als eine anzuwendende Methodik vorsieht.

1 Formale Aspekte

Tabelle 3: Formale Aspekte.

Aspekt	Beschreibung
Titel :	IT-Grundschutz-Profil für Weltrauminfrastrukturen – Mindestabsicherung für den Satelliten über den gesamten Lebenszyklus ¹
Autorenschaft:	Siehe Kap. 3 „Liste der Autorinnen und Autoren“
Herausgeberschaft:	BSI, OHB Digital Connect, Airbus CyberSecurity, Deutsche Raumfahrtagentur im DLR
Versionsstand:	Veröffentlicht am 30.06.2022, Version 1.0 Finalisiert im Mai 2022
IT-Grundschutz-Kompendium	Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2022
Revisionszyklus:	Die Aktualität des Dokuments soll 2-jährlich überprüft werden.
Vertraulichkeit:	Das Dokument in der hier vorliegenden Version ist offen zugänglich.

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-Profiles durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

3 Liste der Autorinnen und Autoren

An der Erarbeitung des Dokuments beteiligt waren die Teilnehmerinnen und Teilnehmer der Workshop-Reihe „Mindestanforderungen an die Cybersicherheit für Satelliten“, welche vom BSI veranstaltet und moderiert worden ist. Aus dieser Gruppe bildete sich ein Autoren-Team, dessen Mitglieder in folgender Tabelle aufgelistet sind.

Tabelle 4: Liste der Autorinnen und Autoren.

Name	Organisation
Dr. Johanna Niecknig	Bundesamt für Sicherheit in der Informationstechnik
Wim Fleischhauer	OHB Digital Connect GmbH (zeitweise)
Manuel Hoffmann	OHB Digital Connect GmbH
Miriam Goellner	Airbus CyberSecurity GmbH

Alle weiteren an der Erstellung dieses Profils Beteiligten, welche an verschiedenen Arbeitspaketen (z.B. zur Strukturanalyse, Modellierung, Erstellung der Checkliste) mitgewirkt haben, in ergiebigen Diskussionen ihre Expertise beisteuerten und dieses Profil Korrektur gelesen haben, finden sich in der nachfolgenden Tabelle wieder.

¹ Zur genauen Abgrenzung siehe Kapitel 6.1.

Tabelle 5: Liste der weiteren Beteiligten an der Erstellung des IT-Grundschutz-Profiles

Name	Organisation
Birger Klein	Bundesamt für Sicherheit in der Informationstechnik
Wendel Lohmer	Bundesamt für Sicherheit in der Informationstechnik
Frank Christophori	Bundesamt für Sicherheit in der Informationstechnik
Stefanie Grundner	PanaGlobo - Geospatial Consultancy
Dr. Sabine Philipp-May	Deutsche Raumfahrtagentur im DLR
Johannes Stahl	Deutsche Raumfahrtagentur im DLR
Lukas Ellenrieder	Airbus Defence and Space GmbH
Erwin Hirschmüller	Airbus Defence and Space GmbH
Karel Kotarowski	Airbus Defence and Space GmbH
Prof. Dr. Steffen Kuntz	Airbus Defence and Space GmbH
Andreas Kopper	Airbus CyberSecurity GmbH
André Penzien	OHB Digital Connect GmbH
Niek van Dael	OHB System AG

4 Management Summary

4.1 Zielgruppe

Das IT-Grundschutz-Profil für Satelliten richtet sich an die für die Informationssicherheit Verantwortlichen in Raumfahrteinrichtungen (Herstellung und Betrieb von Satelliten), siehe Kap. 5.1.

4.2 Zielsetzung

Dieses IT-Grundschutz-Profil soll den Anwendern helfen, Informationssicherheit in allen den Lebenszyklus des Satelliten betreffenden Prozessen zu gewährleisten und an die satellitenspezifischen Bedürfnisse anzupassen. Es soll als Schablone dienen, den IT-Grundschutz des BSI in geeigneter Weise zu implementieren.

Dieses IT-Grundschutz-Profil definiert ein empfohlenes Mindest-Schutzniveau für die Informationssicherheit bei Satelliten, welches während des gesamten Lebenszyklus des Satelliten berücksichtigt werden sollte. Dazu werden Geschäftsprozesse, die sich am Lebenszyklus des Satelliten orientieren, definiert. Entsprechend der Herangehensweise der Standard-Absicherung nach IT-Grundschutz werden Sicherheitsanforderungen, die erfüllt werden sollten, beschrieben. Die untersuchten Geschäftsprozesse sind:

- Konzeption und Design
- Herstellung
- Test
- Transporte
- Inbetriebnahme
- Betrieb

- Außerbetriebnahme

Zusätzlich wurde eine Gemeinsame IT-Infrastruktur als ein Querschnittsprozess definiert, der IT-Infrastrukturen konzentriert, die in allen oben genannten Prozessen verwendet werden. Dieser Querschnittsprozess vereinfacht die Anwendung des BSI Grundschutzes innerhalb des Grundschutz-Profils.

Das BSI empfiehlt die Anwendung dieses IT-Grundschutz-Profils als Einstieg in eine Informationssicherheitskonzeption. Die tatsächliche Anwendung der empfohlenen Anforderungen ist missionsabhängig zu überprüfen.

Für zahlreiche Satellitensysteme wird ein höherer Schutzbedarf zugrunde zu legen sein, der die Anwendung von Anforderungen über die hier beschriebene Mindestabsicherung hinaus notwendig macht. Gleichmaßen kann es in Einzelfällen vorkommen, dass ein Anwender des Profils entscheidet, gewisse Maßnahmen nicht umzusetzen. Diese Entscheidungen sollten möglichst durch eine Risikobetrachtung unterlegt sein.

4.3 Aufgaben der Leitungsebene

Die Autorinnen und Autoren empfehlen der Leitungsebene von Einrichtungen aus dem Raumfahrtbereich die Anwendung dieses IT-Grundschutz-Profils als Grundlage für das Informationssicherheitskonzept bei der Herstellung und dem Betrieb von Satelliten (in Ergänzung zu etablierten terrestrischen Anforderungen für das Bodensegment und die allgemeinen Infrastrukturen).

Die Autorinnen und Autoren weisen zudem auf eine angemessene Berücksichtigung und Handhabung von Informationssicherheits-Risiken in der Supply Chain hin. Daher ist durch die Leitungsebene dafür Sorge zu tragen, dass, neben der für den Schutzbedarf notwendigen Absicherung nach IT-Grundschutz der Supply Chain, der Zulieferer angemessen nach dessen Vertrauenswürdigkeit ausgewählt werden.

Im Falle eines Outsourcings von IT oder Prozessen empfehlen die Autorinnen und Autoren, die entsprechenden Dienstleister zu verpflichten, eine Mindestabsicherung (z.B. auf Grundlage dieses IT-Grundschutz-Profils) nachzuweisen.

5 Festlegung des Geltungsbereichs

5.1 Zielgruppe

Das IT-Grundschutz-Profil für Satelliten richtet sich an die für die Informationssicherheit, die Informationstechnik, die Infrastruktursicherheit verantwortlichen Entscheidungsträger und Projektleiter der Einrichtungen aus dem Raumfahrtbereich (Herstellung und Betrieb von Satelliten). Der Fokus liegt dabei auf dem Satelliten selbst, während die zugehörige Bodeninfrastruktur oder auch das Startsegment, die Supply Chain etc. in diesem Profil nicht vollumfänglich betrachtet wird². Gleichzeitig soll es auch Herstellern und Lieferanten in der Supply Chain von Komponenten für den Einsatz im Satelliten als Grundlage für die Absicherung des Aufbaus und der Entwicklung ihrer Systeme und Anwendungen dienen.

² Es ist davon auszugehen, dass für das Bodensegment IT-Grundschutz ohne raumfahrtspezifische Besonderheiten anwendbar ist und somit eine etablierte Grundabsicherung gegeben ist. Schnittstellen, die direkt zum Satelliten gehen und somit Satellitenspezifika aufweisen, sind in diesem Profil mit aufgenommen.

5.2 Beschreibung des Schutzbedarfs

Die Ermittlung des Schutzbedarfs bei Satellitensystemen erfolgt missionsabhängig, d.h. der Schutzbedarf ist abhängig von Aufgabe, Größe und Kritikalität der geplanten Mission. Je nach Mission kann somit ein niedriger bis sehr hoher Schutzbedarf vorliegen.

Da es sich bei dem vorliegenden IT-Grundschutz-Profil um Empfehlungen zu einer *Mindestabsicherung* handelt, die für alle Satelliten anwendbar sein sollen, wurde in einer generischen Schutzbedarfsanalyse anhand von fünf Beispielmissionen, welche in Kap. 9.1.3 definiert sind, der niedrigste Schutzbedarf ermittelt. Dazu wurden einerseits für die verschiedenen Beispielmissionen die für die Informationssicherheit relevanten Szenarien abgeleitet. Andererseits wurden regulatorische Anforderungen aus Normen, Standards und Gesetzen untersucht.

Ausgehend von den Beispielmissionen mit den geringsten Schadensauswirkungen konnten keine Szenarien identifiziert werden, die die Schutzbedarfskategorie „Normal“ überschreiten.

Für das vorliegende IT-Grundschutz-Profil ist daher der Schutzbedarf „Normal“ für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit als Mindest-Schutzbedarfsniveau angesetzt worden. Infolgedessen wird in diesem IT-Grundschutz-Profil ein Schutzniveau mit mindestens einer Standard-Absicherung der IT-Grundschutz-Vorgehensweise angestrebt.

5.3 IT-Grundschutz Vorgehensweise

Der IT-Grundschutz des BSI bietet die Vorgehensweisen Basis-, Standard oder Kern-Absicherung an. Abhängig von der gewählten Vorgehensweise müssen die in den Bausteinen beschriebenen Anforderungen umgesetzt werden. Die beschriebenen Anforderungen in diesem IT-Grundschutz-Profil entsprechen mindestens der Standardabsicherung des BSI-Standards 200-2. Diese entspricht der empfohlenen IT-Grundschutz-Vorgehensweise. Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel und kann auch als Basis für ein höheres Schutzniveau dienen. Da für jede Satellitenmission der Schutzbedarf individuell festzustellen ist, wird empfohlen, an die Mission angepasst einzelne Anforderungen aus dem erhöhten Schutzbedarf ebenfalls umzusetzen.

5.4 Kompatibilität zu anderen Standards

Durch eine Umsetzung der Standard-Absicherung besteht Kompatibilität zu ISO 27001³. Ferner sind jene Anforderungen, die über die Bausteine des IT-Grundschutzes hinausgehen, angelehnt an gängige Standards im Bereich Raumfahrt und IT-Sicherheit, wie z.B. Standards der CCSDS, ECSS und NIST.

5.5 Berücksichtigte Rahmenbedingungen

Fallen Betreiber- und Herstellereinrichtungen unter die KRITIS- oder UBI-Verordnung, bestehen gemäß §8a bzw. §8f BSI-Gesetz Pflichten für die Einrichtungen, wie z.B. die Meldung von IT-Störungen bzw. Sicherheitsvorfällen oder die Absicherung der Systeme nach dem aktuellen Stand der Technik bzw. eine Verpflichtung zur Selbsterklärung zur IT-Sicherheit. Hierbei beschränkt sich die KRITIS-Verordnung jedoch auf das Bodensegment ausgewählter Missionen⁴. Für Satellitenmissionen existieren aktuell keine

³ <https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716> (aufgerufen am 01.07.2019)

⁴ Nach der BSI-KritisV im Anhang 7 Teil 3 Nr. 1.7.2 existiert nur folgender Bereich als Kritische Infrastruktur (Stand 2022): 1.7.2. Bodenstation eines Satellitennavigationssystems (Bemessungskriterium: Einordnung der Anlage nach der Verordnung (EU) Nr. 1285/2013) (Schwellenwert: Bodenstation)

spezifischen gesetzlichen Rahmenbedingungen oder verbindlich anwendbare Normen für die Informationssicherheit.

6 Abgrenzung des Informationsverbundes

Die zusammenhängenden Komponenten einer Institution oder eines speziellen Anwendungsbereichs werden als Informationsverbund bezeichnet. Im nächsten Abschnitt werden die für das IT-Grundschutz-Profil relevanten Bestandteile des Informationsverbunds „Satellit“ definiert. Anschließend werden die Teile des Informationsverbundes aufgeführt, die in diesem IT-Grundschutz-Profil nicht berücksichtigt werden.

6.1 Bestandteile des Informationsverbundes

Zum Informationsverbund „Satellit“ gehören alle Prozesse und Verfahren, die während des gesamten Lebenszyklus für den Satelliten direkt oder über Schnittstellen relevant sind, sowie alle technischen Bestandteile wie Anwendungen, IT-Systeme, Räume und Gebäude, die diese Prozesse und Verfahren unterstützen.

6.2 Nicht berücksichtigte Teile

Der Fokus dieses Profils liegt auf dem Satelliten selbst. Daher ist das Bodensegment, etwa das Bodenkontrollzentrum, oder Supportinfrastrukturen, z.B. für den Satellitenstart, nicht vollumfänglich aufgenommen und es wird lediglich die Schnittstelle, die direkt mit der Informationssicherheit des Satelliten in Bezug steht, in den Informationsverbund mit aufgenommen. Der Hersteller/Betreiber eines Systems ist jedoch angehalten darauf zu achten, dass auch in diesen Einrichtungen ein vergleichbares Sicherheitsniveau durch deren Betreiber nachgewiesen werden kann.

7 Referenzarchitektur

Die Referenzarchitektur legt fest, welche Anwendungen, IT-Systeme und räumlichen Infrastrukturen (Räume, Gebäude, Satellit, Weltall) für die wesentlichen Prozesse im Lebenszyklus eines Satelliten relevant sind und im Sinne des IT-Grundschutzes abgesichert werden sollten. Die im Folgenden dargestellte Referenzarchitektur und Prozesse sollten in adäquat angepasster Form auch für andere Modelle, z.B. EM, FlatSat, der Satellitenentwicklung angewendet werden.

7.1 Prozesse

Die Geschäftsprozesse, die in diesem IT-Grundschutz-Profil aufgegriffen werden, orientieren sich an den Phasen, die ein Satellit in seinem Lebenszyklus⁵ durchläuft. Im Folgenden werden diese Prozesse kurz beschrieben und mit einem Identifikator versehen.

G00 Gemeinsame IT-Infrastruktur

Ergänzend zu den am Lebenszyklus des Satelliten orientierten Phasen ist hier ein Querschnittsprozess definiert, der übergreifend die gemeinsame IT-Infrastruktur beschreibt. Hier sind allgemeine IT-Infrastrukturen, die in allen Geschäftsprozessen genutzt werden, zusammengefasst.

⁵ Die gewählten Lebensphasen sind gegenüber den Definitionen nach ECSS-Standards nach Praktikabilität zusammengefasst oder durch weitere Phasen/Prozesse ergänzt.

G01 Konzeption und Design

Alle auf die Herstellungsphase vorbereitenden Aktivitäten (System-Analyse, System-Definition, System-Design, Missionsanalysen insbesondere Risikoanalysen etc.), bis zur vollständigen Definition des Systems sind in diesem Prozess zusammengefasst. Ausgenommen sind technische Vorentwicklungen.

G02 Herstellung

Im Prozess „Herstellung“ werden Entwicklungen von Hardware und Software, Integration und Zusammenbau aller Komponenten, sowie die Umsetzung der entsprechenden Sicherheitsanforderungen betrachtet. Dieser Prozess umfasst auch notwendige Vorentwicklungen (inkl. SCM Management), sowie Zwischentests/Integrationstests (Labortests).

G03 Test

Diese Phase umfasst funktionale Tests und Qualifikationstests. Ebenso werden in diesem Prozess die Umwelttests betrachtet, welche durchgeführt werden, um sicherzustellen, dass der Satellit auch nach dem Start unter Weltraumbedingungen einwandfrei funktioniert.

G04 Transporte

In diesem Prozess wird der Transport des Satelliten sowie spezieller Komponenten (z.B. der Kryptoeinheit) betrachtet, etwa zu Umwelttests oder zum Startplatz. Ebenso wird die Lieferung der Systemkomponenten berücksichtigt.

G05 Inbetriebnahme

Der Prozess „Inbetriebnahme“ beinhaltet die Vorbereitung des Satellitenstarts. Zu diesen Vorbereitungen gehören insbesondere die finalen Checks und ggf. die Aktivierung der Instrumente, Sicherstellung des Checks der Startrakete sowie aller für den Start benötigten Einrichtungen, das Keying, sowie der Start des Satelliten in die Erdumlaufbahn. Ebenso ist die Launch and Early Orbit Phase Teil dieses Prozesses. Die Inbetriebnahme wird typischerweise mit dem Commissioning Results Review bzw. einem Flight Qualification Review abgeschlossen.

G06 Betrieb

Diese Phase beschreibt den operationellen Einsatz des Satelliten. Der Prozess umfasst typischerweise folgende Unterprozesse: Überwachung, Wartung, Qualitätskontrolle der Datenströme, Kommandoübertragung, Kommandoimplementierung, Annahme von Steuerungsdaten von Kontrollzentrum.

G07 Außerbetriebnahme

In dieser Phase wird die Außerbetriebssetzung des Systems durchgeführt.

7.2 Anwendungen

Zum Informationsverbund gehören neben den Prozessen auch die Anwendungen, die eine Bearbeitung der Prozesse unterstützen. Dies sind im Lebenszyklus des Satelliten neben allgemeinen Anwendungen bzw. Diensten (z.B. E-Mail-Service oder Datenaustausch-Dienst) auch die für die Raumfahrt spezifischen Anwendungen und Dienste (bspw. Analyse-Tools, EGSE, Simulatoren), sowie Anwendungen, Komponenten und Geräte und Dienste, die sich an Bord des Satelliten befinden (z.B. Plattform, Payload, SAT Controller). Diese oben angesprochenen Anwendungen sind in der folgenden Tabelle mit einem Identifikator aufgeführt. In der rechten Spalte ist angegeben, welche Prozesse von den Anwendungen unterstützt werden.

Tabelle 6: Anwendungen des Informationsverbundes „Satellit“

Identifikator	Anwendungen des Informationsverbundes	Unterstützte Prozesse
A101	Verzeichnisdienst	G00
A102	Storagedienst	G00
A103	DNS-Dienst	G00
A104	Zentraler Zeitservice	G00
A105	Web-Service	G00
A106	File-Service	G00
A107	Virtualisierungsservice	G00
A108	Containerisierungsservice	G00
A109	Datenaustausch-Dienst	G00
A110	Telefonie	G00
A111	Druckservice	G00
A113	Mobiltelefonie	G00
A114	E-Mail-Service	G00
A115	Office inkl. Video- und E-Mail-Client	G00
A201	CAD Server	G01, G02
A202	CAD Client/Standalone	G01, G02
A203	Ticket-System Server	G01, G02, G03, G05, G06, G07
A204	Ticket-System Client	G01, G02, G03, G05, G06, G07
A205	DMS-KonfigMgmt Server	G01, G02, G03, G05, G06
A206	DMS-KonfigMgmt Client	G01, G02, G03, G05, G06
A207	Quellcodeverwaltung, BuildChain, UnitTests Server	G01, G02, G03
A208	IDE Client/Standalone	G01, G02, G03
A209	Requirement-Eng/Mgmt Server	G01, G02, G03
A210	Requirement-Eng/Mgmt Client	G01, G02, G03
A211	Analyse-Tools	G01, G02, G03, G05, G06, G07
A212	ERP Server	G02
A213	ERP Client	G02
A214	Soft-/Hardware Test Tools	G02, G03, G05, G06
A215	Simulatoren	G02

Identifikator	Anwendungen des Informationsverbundes	Unterstützte Prozesse
A216	Fertigungssysteme	G02
A217	Checkout-System	G02, G03, G05
A218	EGSE	G02, G03, G04, G05
A219	MGSE	G02, G03, G04, G05
A220	Anwendungen/Tools des Test-Centers	G03
A221	Transportcontainer Software	G04
A301	Sat ASW Plattform	G02, G03, G04, G05, G06, G07
A302	Sat ASW Payload	G02, G03, G04, G05, G06, G07
A303	SAT Control Unit/Controller	G02, G03, G04, G05, G06, G07
A304	SAT Kommunikation	G02, G03, G04, G05, G06, G07
A305	SAT GNSS	G02, G03, G04, G05, G06, G07
A306	SAT Autonomie Systeme	G05, G06, G07

A101-A115 sind Allgemeine Anwendungen und Dienste, A201 - A221 Spezifische Anwendungen und Dienste und A301 – A306 Satellitenspezifische Anwendungen und Dienste.

7.3 IT-Systeme

Tabelle 7: IT-Systeme des Informationsverbundes „Satellit“

Identifikator	IT-Systeme des Informationsverbundes	Abhängige Anwendungen	Abhängige Prozesse
S101	Storageplattform	A101	G00
S102	DNS	A102	G00
S103	Zeitsynchronisation	A103	G00
S104	Webserver	A104	G00
S105	Fileserver	A105	G00
S106	Virtualisierungsplattform	A106	G00
S107	Containerplattform	A107	G00
S108	Win/Linux/DB	A108	G00
S109	Datenaustauschserver Win/Linux/DB	A109	G00
S110	TK-System	A110	G00
S111	Druckserver Win/Linux	A111	G00
S112	Drucker	-	-
S114	E-Mail-Server Win/Linux	A114	G00

S115	Office-Client alle OS, Tablet, Laptop und Desktop	A115	G00
S201	Win/Linux/DB	A201	G01, G02
S202	CAD Client Win/Linux, Laptop und Desktop	A202	G01, G02
S203	Win/Linux/DB	A203	G01, G02, G03, G05, G06, G07
S204	Ticket Client Win/Linux, Laptop und Desktop	A204	G01, G02, G03, G05, G06, G07
S205	Win/Linux/DB	A205	G01, G02, G03, G05, G06
S206	DMS-KonfigMgmt Client Win/Linux, Laptop und Desktop	A206	G01, G02, G03, G05, G06
S207	Win/Linux/DB	A207	G01, G02, G03
S208	IDE Client alle OS, Laptop und Desktop	A208	G01, G02, G03
S209	Win/Linux/DB	A209	G01, G02, G03
S210	Requirement Client Win/Linux, Laptop und Desktop	A210	G01, G02, G03
S211	Analyse-Tool Client Win/Linux, Desktop, Laptop, Tablet	A211	G01, G02, G03, G05, G06, G07
S212	ERP Server Win/Linux/DB	A212	G02
S213	ERP Client Win/Linux, Desktop	A213	G02
S214	Proprietäre Systeme teilweise auf Basis Win/Linux/RT-OS, ggf. Laptop, Tablet	A214	G02, G03, G05, G06
S215	Proprietäre Systeme teilweise auf Basis Win/Linux/RT-OS	A215	G02
S216	Proprietäre Systeme teilweise auf Basis Win/Linux/RT-OS, ggf ergänzt um proprietäre und offene Prozessleittechnik	A216	G02
S217	Win/Linux/DB	A217	G02, G03, G05
S218	EGSE Hardware mit Controller-PC Win/Linux, ggf. Laptop, Tablet	A218	G02, G03, G04, G05
S219	Proprietäre Systeme von proprietärer Microcontroller Basis bis Industrie-PC mit Win/Linux/RT-OS, ggf. Laptop, Tablet	A219	G02, G03, G04, G05
S220	Proprietäre Systeme teilweise auf Basis Win/Linux/RT-OS	A220	G03
S221	Proprietäre Systeme von proprietärer Microcontroller Basis	A221	G04
S301	On-Board Computer Plattform mit RT-OS (Prozessor Modul)	A301	G02, G03, G04, G05, G06, G07
S302	On-Board Computer Payload mit RT-OS (Prozessor Module)	A302	G02, G03, G04, G05, G06, G07
S303	Microcontroller	A303	G02, G03, G04, G05, G06, G07

S304	Telemetry Tracking & Command System (TT&C), Crypto Unit, On-Board Computer / Data Handling System	A304	G02, G03, G04, G05, G06, G07
S305	Proprietärer Controller	A305	G02, G03, G04, G05, G06, G07
S306	On-Board Computer Plattform mit RT-OS (Prozessor od. Spezial Modul)	A306	G05, G06, G07

7.4 Netze und Netzkomponenten

Anwendungen und IT-Systeme des Informationsverbundes „Satellit“ sind in verschiedene Netzwerke eingebunden. Auch wenn sich Anzahl und Aufbau der Netze nicht im Detail verallgemeinern lassen, wird davon ausgegangen, dass die Architektur vieler Beispielmmissionen hinsichtlich Netzen und Netzkomponenten zumindest ähnlich ist.

Aus diesem Grund wurden für die Architektur einer Beispielmmission einzelne Bausteine ausgewählt, die im Rahmen des Informationsverbundes „Satellit“ umgesetzt werden sollen. Es handelt sich hierbei um System-Bausteine der Schicht NET, welche Vernetzungsaspekte im Zusammenhang mit Netzverbindungen und Kommunikation miteinschließt.

Die folgenden Bausteine der Schicht NET wurden ausgewählt:

- Netzarchitektur und -design (NET.1.1)
- Netzmanagement (NET.1.2)
- WLAN-Betrieb (NET.2.1)
- WLAN-Nutzung (NET.2.2)
- Router und Switches (NET.3.1)
- Firewall (NET.3.2)
- VPN (NET.3.3)

Der Baustein Netzarchitektur und -design wird auf das Gesamtnetz einer Beispielmmission inklusive aller Teilnetze angewandt. Teilnetze des Informationsverbundes „Satellit“ sind beispielsweise das Teilnetz des Serverraums oder das Teilnetz des Büroraums, wie in der Abbildung des Netzplans in Abschnitt 8.4.1 zu erkennen ist.

Neben dem Baustein Netzarchitektur und -design wird auch der Baustein Netzmanagement auf den vorliegenden Informationsverbund angewandt. Im Rahmen des Netzmanagements werden die verschiedenen Netzkomponenten umfassend integriert. Es werden ebenso geeignete Maßnahmen umgesetzt, um die Kommunikation und Infrastruktur des Netzmanagements zu schützen.

Weitere relevante Bausteine sind die Bausteine WLAN-Betrieb und WLAN-Nutzung. WLAN-Betrieb und WLAN-Nutzung sind in den Teilnetzen der Satellitenintegration, des Launch-Centers und des Test-Centers vorgesehen, wo beispielsweise mittels mobiler Endgeräte die Integration des Satelliten überwacht oder gesteuert werden kann.

Netzkomponenten werden ebenfalls als Teil des Informationsverbundes betrachtet, weshalb der Baustein Router und Switches sowie der Baustein Firewall der Schicht NET ausgewählt wurden. Router und Switches sind nicht im Netzplan abgebildet, da sich der Aufbau der IT-Infrastruktur von Mission zu Mission unterscheidet. Abgebildet sind jedoch Firewalls und Schlüsselgeräte zur Segmentierung des Gesamtnetzes und zur Herstellung einer VPN-Verbindung.

7.5 Gebäude und Räume

Nicht nur die informationstechnischen Komponenten spielen bei der Informationssicherheit eine große Rolle. Auch die Sicherheit der Gebäude und Räume, in denen der Satellit oder mit dem Lebenszyklus des Satelliten verknüpfte Systeme oder Komponenten hergestellt, getestet, transportiert und betrieben werden oder Mitarbeitende tätig sind, ist bei einer Absicherung nach IT-Grundschutz zu berücksichtigen. Für den Satelliten ergibt sich die Besonderheit, dass der Satellit selbst auch als „Raum“, der Weltraum als „Gebäude“ betrachtet werden kann.

Tabelle 8: Räume des Informationsverbundes „Satellit“

Identifikator Räume	Räume des Informationsverbundes	Identifikator Gebäude	Gebäude des Informationsverbundes	In den Räumen installierte IT-Systeme oder durchgeführte Prozesse
R01	Büro 1	G01	Gebäude 1	S112, S114, S202, S204, S206, S208, S210, S211, S213
R02	Serverraum	G02	Gebäude 2	S101, S102, S103, S104, S105, S106, S107, S108, S109, S110, S111, S114, S201, S203, S205, S207, S209, S212, S215
R03	Satellitenintegrationsraum / -halle	G03	Integrationsgebäude	S214, S216, S217, S218, S219, S301, S302, S303, S304
R04	Testraum / -halle	G04	Test-Center	S214, S217, S218, S219, S220
R05	Launch-Halle	G05	Launch-Center	S214, S217, S218, S219
R06	Rack/Transportcontainer	G06	Transportcontainer (LKW, Flugzeug)	S218, S221
R07	Satellit	G07	Weltraum	S214, S301, S302, S303, S304, S305, S306
R07	Satellit	G03, G04	Integrationsgebäude, Test-Center	S214, S301, S302, S303, S304, S305
R07	Satellit	G05	Launch-Center	S301, S302, S303, S304, S305, S306
R07	Satellit	G06	Transportcontainer (LKW, Flugzeug)	S301, S302, S303, S304

7.6 Annahmen und Erläuterungen

Im Folgenden werden die im Rahmen der Strukturanalyse zur Auswahl der Referenzarchitektur getroffene Annahmen zusammengefasst und weiterführende Erläuterungen zu verschiedenen Zielobjekten gegeben.

- Systeme, wie z.B. E-Mail-Server, werden - auch innerhalb eines Geschäftsprozesses - mehrfach vorhanden sein, da es i.d.R. mehrere bzw. viele beteiligte Unternehmen innerhalb eines Geschäftsprozesses gibt. Jedoch würden mehrfache Systeme im Informationssystem keinen Mehrwert generieren, da keine Besonderheiten im Gegensatz zu einer Vereinfachung zu erwarten sind.
- Es werden allgemeine Services (u.a. Server) genutzt, um ein breiteres Spektrum abzudecken. Beispielsweise wird der Begriff „Email-Server“ genutzt statt konkrete Produkte wie Exchange, Postfix

oder Notes in der Analyse (und der Modellierung) zu nennen. Bei der Anwendung des IT-Grundschutz-Profils in der Praxis ist die Strukturanalyse um die konkreten Services bzw. Produkte zu ergänzen.

- Testaktivitäten sind in mehreren Geschäftsprozessen verortet, da sie zu unterschiedlichen Zeitpunkten mit unterschiedlichen Mitteln und Zielen durchgeführt werden.
- Für Anwendungen und IT-Systeme, die in verschiedenen Geschäftsprozessen auftauchen, werden gleiche ID's vergeben. Grund dafür ist die Annahme, dass es für die überwiegende Anzahl der Systeme geschäftsprozess-übergreifend keine Änderungen gibt.
- Container werden nicht bezüglich ihres Einsatzes unterschieden. Falls im Rahmen der Schutzbedarfsanalyse und -vererbung unterschiedliche Einsatzfelder mit unterschiedlichen Schutzbedarfen identifiziert werden, kann eine Erweiterung vorgenommen werden.
- Für die Satellitenkomponenten wird der Satellit als Raum betrachtet und der Weltraum als Gebäude (nach dem Start). So können unterschiedliche Phasen (am Boden, Transport, im Weltraum) unterschieden und unterschiedliche Bedrohungen/Maßnahmen des Einsatzortes abgebildet werden.
- Office verbleibt als Kommunikationsmittel im Geschäftsprozess "Betrieb", da z.B. zwischen Betreiber und Hersteller Informationen über Störungen ausgetauscht werden müssen.
- Die Umsetzungen von Prozess- bzw. Programmlogik als Software oder als Hardware (z.B. FPGA) werden nicht betrachtet, sondern der allgemeine Fall, die Implementierung als Software, wird betrachtet.
- Die Supply Chain Security wird in der Strukturanalyse nicht detailliert betrachtet. Diese ist im Detail in der Praxis abzubilden. Hierzu gehören u.a. Risiken manipulierter Bauteile wie FPGAs, Microcontroller, sonstige ICs, Software, etc.
- Das Outsourcing von Teilen oder kompletter IT bzw. Prozessen wird nicht explizit dargestellt, ist jedoch für alle IT bzw. Prozesse denkbar und möglich. Das gleiche gilt für die Nutzung von Cloud-Services.
- Bei der Anwendung „Mobiltelefonie“ sind die Zielobjekte IT-Systeme, Räume und Gebäude nicht weiter aufgeführt bzw. spezifiziert, da zum einen der Einfluss des Informationseigentümers auf den Mobilfunkbetreiber gering ist, zum anderen der Einfluss auf die Modellierung gering eingeschätzt wird.
- IDE: Der Einsatz einzelner IDEs ist inzwischen selten. IDE wurde um weitere Komponenten ergänzt, z.B. Quellcodeverwaltung, Build-Chain, Unit Tests, usw.
- Telefonie/TK: Das TK-System umfasst sowohl Soft- und Hardphones auf VOIP-Basis als auch TK-Server bzw. klassische TK-Anlagen mit klassischen Nebenstellen.
- Transportcontainer für SAT und Komponenten werden nicht als EGSE/MGSE betrachtet, sondern als mobile Räume mit Klima-, Alarm und Haustechnik. Die Container können dazu Stromgeneratoren enthalten bzw. daran angeschlossen werden.
- Transportcontainer Software: In Transportcontainern eingesetzte Software dient beispielsweise der Klimatisierung, Transportlokalisierung, Alarmierung oder der Sicherstellung der Energieversorgung.
- Ticket-System: Ein Ticket System besteht i.d.R. aus einem zentralen Server- und einem Clientanteil. Server werden i.d.R. auf Basis von Linux oder Windows betrieben und haben eine offene (z.B. SQL) oder eine proprietäre Datenbank. Bei webbasierten Ticketsystemen besteht der Clientanteil aus einem Clientsystem mit Browser. Hier wäre kein dediziertes Clientsystem notwendig. Der Begriff wird allgemein genutzt und es werden keine konkreten Produkte, z.B. Jira oder OTRS, abgebildet.
- DMS-KonfigMgmt (Dokumentenmanagement inkl. Konfigurationsmanagementsystem): Ein Dokumentenmanagement inkl. Konfigurationsmanagementsystem besteht i.d.R. aus einem zentralen Server- und einem Clientanteil. Server werden i.d.R. auf Basis von Linux oder Windows betrieben und haben eine offene (z.B. SQL) oder eine proprietäre Datenbank. Bei webbasierten DMS-Systemen besteht der Clientanteil aus einem Clientsystem mit Browser. Hier wäre kein dediziertes Clientsystem

notwendig. Der Begriff wird allgemein genutzt und es werden keine konkreten Produkte, z.B. Eclipse oder Sapienza, abgebildet.

- Prototyping und Software-Entwicklung: Beim Prototyping und der Softwareentwicklung werden Entwicklungsumgebungen (IDE) auf Clients in Verbindung mit zentralen Quellcodeverwaltungen, Build- und Unit-Test-Systemen betrieben. Typische Serverumgebungen werden auf Basis von Linux oder Windows betrieben und haben eine offene (z.B. SQL) oder eine proprietäre Datenbank.
- Requirement-Eng/Mgt (Requirement Engineering und Management Systeme): Ein Requirement Engineering und Management System besteht i.d.R. aus einem zentralen Server- und einem Clientanteil. Server werden i.d.R. auf Basis von Linux oder Windows betrieben und haben eine offene (z.B. SQL) oder eine proprietäre Datenbank. Bei webbasierten Requirement-Systemen besteht der Clientanteil aus einem Clientsystem mit Browser. Hier wäre kein dediziertes Clientsystem notwendig. Der Begriff wird allgemein genutzt und es werden keine konkreten Produkte, z.B. Doors, abgebildet.
- ERP (Enterprise Resource Planning, hier insbesondere produktionsplanende und produktionsbekleidende Anwendungen): ERP-Systeme bestehen i.d.R. aus einem zentralen Server- und einem Clientanteil. Server werden i.d.R. auf Basis von Linux oder Windows betrieben und haben eine offene (z.B. SQL) oder eine proprietäre Datenbank. Bei webbasierten ERP-Systemen besteht der Clientanteil aus einem Clientsystem mit Browser. Hier wäre kein dediziertes Clientsystem notwendig. Der Begriff wird allgemein genutzt und es werden keine konkreten Produkte, z.B. SAP, abgebildet.
- SAT ASW (anwendungsspezifische Satellitensoftware Plattform und Payload): Anwendungssoftware für die Payload kann bei kleinen Missionen auf dem On-Board Computer (OBC, speziell Prozessormodul) der Plattform integriert sein. Bei größeren Anforderungen bzw. Missionen kann ein eigenständiger OBC bzw. Prozessormodul für die Payload vorgesehen werden.
- SAT Kommunikation: Die SAT Kommunikation(ssoftware) kann in verschiedenen Units eines Satelliten integriert sein: Telemetry Tracking & Command System (TT&C), Crypto Unit, On-Board Computer / Data Handling System. Bei spezifischen Payloads (z.B. Telekom-Sat) hat die Payload dedizierte Systeme für die SAT Kommunikation.
- SAT Control Unit/Controller: In Subsystemen (z.B. Thermal, Power) können Microcontroller eingesetzt sein, die z.B. Sensordaten dezentral verarbeiten und Aktionen auslösen.
- Checkout-System: Das Checkout-System wird ggf. auch beim Start für z.B. das Aufladen der Batterien genutzt. Beispiele für Checkout-Systeme: Terma CCS, SCOS-2000.
- EGSE: EGSE-Systeme bestehen häufig aus Custom-Hardware mit EGSE Controller auf der Basis eines Industrie-PCs mit Win/Linux. Beispiele für EGSE-Systeme: S-Band SCOE, Ka-Band SCOE, EPS SCOE, AOCS SCOE, PL SCOE, Crypto SCOE.
- MGSE: In Abgrenzung zu EGSE-Systemen handelt es sich bei MGSE hauptsächlich um mechanische Hilfsmittel, die aber über elektronische und ggf. vernetzte Steuerungen verfügen. Beispiele: Trolley, Kräne mit vernetzter Steuerung.
- Soft-/Hardware Test Tools: Beispiele für Soft-/Hardware Test Tools sind vernetzbare Oszilloskope oder digitale Multimeter.
- Simulatoren: Simulatoren werden i.d.R. im Entwicklungsnetzwerk verwendet. Simulatoren in den Integrationshallen werden durch EGSE dargestellt. Beispiele für Simulatoren: Flugdynamik mit MATLAB, Simulink, AGI's Systems ToolKit (STK), ESA's godot, GMAT, Orekit.
- Crypto Hardware/Software: Hierunter können dedizierte Geräte, Einschübe in den OBC, integriert in TM/TC-Einschübe oder andere Lösungen verstanden werden.

7.7 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der hier dargestellten Referenzarchitektur ab, sollten die zusätzlichen oder nicht vorhandenen Objekte dokumentiert und begründet werden. Die Objekte sollten passenden Komponenten des IT-Grundschutz Kompendiums zugeordnet werden. Die abgeleiteten Anforderungen sollten an den jeweiligen Schutzbedarf angepasst werden.

8 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Das IT-Grundschutz-Kompendium des BSI stellt Bausteine bereit, die anwendungsbezogene Empfehlungen zur Umsetzung des IT-Grundschutzes geben. Hierzu wird zunächst der Schutzbedarf der Prozesse, Anwendungen, IT-Systeme und Kommunikationsverbindungen festgelegt. Anschließend werden die relevanten Bausteine identifiziert und eine Anpassung der Anforderungen an die entsprechende Zielgruppe durchgeführt. Das Resultat der Anpassung der Anforderungen kann bedeuten, dass alle oder nur bestimmte Anforderungen des Bausteins für die Informationssicherheit in Satelliten bzw. für deren Herstellung und Betrieb relevant sind. Ebenso können Anforderungen als komplett irrelevant eingestuft werden. Auch die Relevanz der in den Anforderungen aufgeführten Maßnahmen sollte identifiziert werden.

Ferner existieren Anforderungen spezifisch für Satelliten, die in den bestehenden IT-Grundschutz-Bausteinen nicht hinreichend modelliert sind. Diese werden am Ende dieses Kapitels aufgeführt. Hier kann eine ergänzende Sicherheitsanalyse erforderlich werden.

8.1 Feststellung des Schutzbedarfs

8.1.1. Rahmenbedingungen

Die Schutzbedarfsanalyse für ein BSI IT-Grundschutz-Profil weicht von einer typischen Schutzbedarfsanalyse für den Informationsverbund einer Einrichtung oder einer Projektumgebung in nachfolgenden Punkten ab:

- Es stehen keine dedizierten Informationseigentümer zur Ermittlung der Schutzbedarfe der betroffenen Informationen zur Verfügung.
- Die Mission und damit Aufgabe, Größe und Kritikalität des Satelliten, ist nicht konkret bekannt und kann ebenfalls nicht zur Ermittlung des Schutzbedarfs herangezogen werden.

Für diese initiale Version des IT-Grundschutz-Profiles werden Maßnahmen für eine *Mindestabsicherung* beschrieben, die für alle Satellitenmissionen anwendbar sein sollen. Daher wird anhand von Beispielmmissionen diejenige mit niedrigstem Schutzbedarf ermittelt. Dieser Schutzbedarf wird zur Erhebung der Mindestanforderungen an Satelliten(-infrastrukturen) zugrunde gelegt.

8.1.2. Methodik

Aufgrund der o.g. Rahmenbedingungen wird ein Top-Down-Ansatz verwendet, der unterschiedliche Beispielmmissionen betrachtet, um eine allgemeine Bewertung der möglichen Schutzbedarfe zu ermöglichen.

Relevanten Szenarien für Weltrauminfrastrukturen und allgemeingültige regulatorische Anforderungen werden mit den Beispielmmissionen in Verbindung gesetzt und die jeweilige Relevanz dargestellt.

Für die Ermittlung des minimalen Schutzbedarfes reicht die Identifikation der Nichtverbindungen und der Verbindungen, die den niedrigsten Schutzbedarf benötigen. Alle weiteren Verbindungen stellen höhere Schutzbedarfe dar und sind für das vorliegende IT-Grundschutz-Profil nicht zu betrachten.

Die angewendeten Prinzipien sind in folgender Tabelle aufgeführt:

Tabelle 9: Anwendung der Prinzipien

Vorgehen	Prinzip
Risikoanalyse, Szenarienableitung und -filterung	Maximalprinzip
Filterung Regulatorik zu Beispielmmissionen	Minimalprinzip
Filterung Szenarien zu Beispielmmissionen	Minimalprinzip
Bewertung innerhalb der finalen Beispielmmission	Maximalprinzip

8.1.3. Beispielmmissionen

Für diese generische Schutzbedarfsanalyse werden verschieden große Beispielmmissionen mit unterschiedlichen Zielsetzungen betrachtet, um die Anwendbarkeit von Szenarien und die potentiellen Schadensauswirkungen dieser zu ermitteln.

Tabelle 10: Beispielmmissionen

Name	Bemerkung
M.01	Für wissenschaftliche Experimente umfasst die Mission einen Kleinstsatelliten, der in eine erdnahe Umlaufbahn gebracht wird und zum Missionsende, idealerweise kontrolliert, Außerdienst gestellt werden.
M.02	Die Mission umfasst einen, mehrere oder viele Telekommunikationssatelliten mit langer Missionsdauer. Die Umlaufbahnen können LEO, MEO und GEO umfassen.
M.03	Kommerzielle ⁶ Mission zur Erdbeobachtung mit langer Missionsdauer. Die Umlaufbahn ist i.d.R. LEO.
M.04	Militärische Mission zur Erdbeobachtung mit langer Missionsdauer. Die Umlaufbahn ist i.d.R. LEO.
M.05	Mission für Navigationssatelliten, die eine Konstellation bilden, eine lange Laufzeit haben und im MEO platziert werden.

8.1.4. Schutzbedarf, Regulatorik und Szenarien

Die Betrachtung der Informationssicherheitsrisiken der betreffenden Parteien wird über Szenarien konkretisiert.

Aufgrund der Allgemeingültigkeit von Anforderungen aus Normen, Standards und Gesetzen wird die Regulatorik separat betrachtet.

8.1.4.1 Schutzbedarf Metrik

Die IT-Grundschutz-Methodik des BSI empfiehlt, zur Einstufung des Schutzbedarfs, diesen qualitativ in drei Kategorien zu unterteilen:

- „Normal“ - N

⁶ Bei den Missionen M.03 und M.04 werden Erdbeobachtungsmissionen für kommerzielle und militärische Zwecke differenziert betrachtet aufgrund grundlegender Unterschiede auf Missionsebene und damit einhergehend zu erwartender Unterschiede bzgl. des Schutzbedarfs. Hingegen wird diese Unterscheidung für Kommunikationssysteme, M.02, für welche es keine so stringente Trennung zwischen militärischer und ziviler/kommerzieller Nutzung gibt, nicht für notwendig erachtet.

- „Hoch“ - H
- „Sehr hoch“ - SH

Grundlegend zur Festlegung des Schutzbedarfs sind die Schadensauswirkungen, die eine Verletzung der Grundziele der Informationssicherheit, Vertraulichkeit, Integrität oder Verfügbarkeit hätten. Die folgende Tabelle bringt die Schutzbedarfskategorien mit den möglichen Schadensauswirkungen in Verbindung:

Tabelle 11: Zusammenhang Schutzbedarfskategorie und Schadensauswirkung

Schutzbedarfskategorie	Schadensauswirkung
Normal	Die Schadensauswirkungen für die Satellitensysteme selbst oder für die Betreiber bzw. Hersteller sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können den Betrieb des Satellitensystems beträchtlich einschränken. Für die Betreiber oder die Hersteller können die Konsequenzen beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können für den Betreiber oder den Hersteller ein existentiell bedrohliches, katastrophales Ausmaß erreichen. Sie können den Betrieb des Satellitensystems stilllegen.

8.1.4.2 Regulatorik

Anforderungen aus Normen, Standards und Gesetzen wirken allgemeingültig auf die betroffenen Parteien. Nachfolgend sind einige ausgewählte, relevante regulatorische Texte und deren Bezug zu den Beispielmmissionen dargestellt:

Tabelle 12: Regulatorik

	M.01	M.02	M.03	M.04	M.05
Satellitendatensicherheitsgesetz (SatDSiG)	-	-	x	-	-
Bundesdatenschutzgesetz (BDSG) / EU GDPR Weitere nationale Datenschutzgesetze (CCPA, PDPB, DPA, usw.)	-	x/partiell	-	-	spez. Dienste
IT-Sicherheitsgesetz 2.0	-	-	-	-	ggf.
EU NIS2-Richtlinie	x/partiell	x/partiell	x/partiell	x/partiell	x/partiell
KRITIS-V	-	-	-	-	x/partiell

8.1.4.3 Szenarien

Aus den Elementargefährdungen und potentiellen Schadenshöhen wurden für das Grundschutz-Profil relevante Szenarien abgeleitet. Diese werden in nachfolgender Tabelle in Beziehung zu den Missionen gebracht. Zusätzlich zu den Szenarien werden die Betroffenen dargestellt.

Tabelle 13: Relevante Szenarien

Betroffene	Szenarien	M.01	M.02	M.03	M.04	M.05
Nutzer/Endkunden	Verfügbarkeit der PL-Information	N	N	N	H/SH	H
Nutzer/Endkunden	Falsche / gefälschte PL-Informationen	N	N	N	H/SH	H
Nutzer/Endkunden	Falsche S/C Rekonfigurierung durch den Nutzer	N	N	N/H	H/SH	

Betroffene	Szenarien	M.01	M.02	M.03	M.04	M.05
Nutzer/Endkunden	Betriebseinschränkung des Nutzers durch Manipulation / Falschnutzung durch andere Nutzer	N	N	N	H/SH	
Satellitenbesitzer	Verlust eigener Satelliten	N	N/H	N/H	H	N
Satellitenbesitzer	Unbefugte Nutzung	N	N	N	H	H
Satellitenbesitzer	Betriebseinschränkung durch bewusste / unbewusste Manipulation	N		N	H	
Satellitenbesitzer	Betriebseinschränkung durch Denial of Service	N	N	N	N/H	H
Satellitenbesitzer	Beeinträchtigung / Beschädigung durch andere Satelliten	N	N	N	H/SH	H
Dritte	Beeinträchtigung / Beschädigung anderer Satelliten durch falschen/fehlerhaften Betrieb	N	N/H	N/H	N/H	N/H

8.1.5. Ergebnis der generischen Schutzbedarfsanalyse

In den vorangegangenen Kapiteln wurden die Beispielmissionen, Szenarien und Regulatorik nach dem Top-Down-Ansatz in Beziehung gebracht.

Die Beispielmission M.01 ist die Mission mit den geringsten Schadensauswirkungen. Bei den Szenarien innerhalb dieser Beispielmission wurden keine Szenarien identifiziert, die die Schutzbedarfskategorie „Normal“ überschreiten.

Für das vorliegende IT-Grundschutz-Profil ist daher der Schutzbedarf „Normal“ für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit als geringster Schutzbedarf anzunehmen.

8.1.6. Hinweise zur Erstellung einer individuellen Schutzbedarfsfeststellung

Das vorliegende IT-Grundschutz-Profil soll Mindestanforderungen für jede Satellitenmission bereitstellen, daher wurde in Kapitel 8.1.5 der minimale Schutzbedarf festgestellt. Bis eine weitere Version eines Grundschutz-Profiles oder Technische Richtlinien zur Verfügung gestellt werden, in welchen neben dem minimalen Schutzbedarf weitere Schutzbedarfsklassen betrachtet werden, um weitere Informationssicherheitsanforderungen für Missionen und Infrastrukturen mit höherem Schutzbedarf unterstützen zu können, sollte der Leser des Profils diesen zusätzlichen Schutzbedarf eigenständig erfassen. Im Falle eines erhöhten Schutzbedarfs („hoch“, „sehr hoch“) für einzelne Zielobjekte ist eine Standard- bzw. Basis-Absicherung nicht ausreichend. Die Anforderungen sollten daher entsprechend angepasst werden, d.h. beispielweise sollten über die Standard-Absicherung hinausgehende Maßnahmen identifiziert und umgesetzt werden. Hilfestellung, wie eine solche unternehmens- und missionspezifische Schutzbedarfsfeststellung zu erstellen ist, bietet im Rahmen einer Schritt-für-Schritt-Anleitung der [Online-Kurs zum IT-Grundschutz](#) (Lektion „[Schutzbedarfsfeststellung](#)“) auf dem Internetauftritt des BSI.

8.2 Auswahl relevanter Bausteinen

Das IT-Grundschutz-Kompendium wird jährlich aktualisiert. Die jeweils aktuelle Fassung veröffentlicht das BSI auf ihrer Homepage⁷.

In den Tabellen Tabelle 14 bis Tabelle 23 wird jeder Baustein aus dem **Kompendium 2022** aufgelistet und auf Relevanz im vorliegenden IT-Grundschutz-Profil überprüft. Sofern ein Baustein nicht relevant ist, wird dies begründet. Dabei kommt das Mindestprinzip zur Anwendung: Es werden nur diejenigen Bausteine modelliert, die für eine Mehrheit der potentiellen Anwender dieses Profils bedeutend sind. Diese Vorgehensweise fokussiert das IT-Grundschutz-Profil auf die wesentlichen und wiederverwendbaren Aspekte. Dies vereinfacht die spätere Umsetzung für die Einrichtungen. Unabhängig davon sollte von den Anwendern des Profils untersucht werden, inwiefern der eigene Informationsverbund vom Profil abweicht. Gegebenenfalls sind bei der späteren Umsetzung weitere Bausteine als relevant einzustufen. Insbesondere ist dabei für viele Missionen ein höherer Schutzbedarf zu betrachten, als der Schutzbedarf der Kategorie „Normal“, der diesem Profil zugrunde gelegt worden ist.

8.2.1. Übergreifende Bausteine (gesamter Informationsverbund)

Tabelle 14 bis Tabelle 19 beinhalten die Bausteine, die übergreifend auf den gesamten Informationsverbund angewendet werden sollten. Diese behandeln ganzheitliche Anforderungen und gelten für sämtliche Teile des Informationsverbundes. Dagegen führen Tabelle 20 bis Tabelle 23 (Kapitel 8.2.2) Systembausteine auf. Systembausteine behandeln die Facetten bestimmter Komponenten. Hier ist entscheidend, ob der Baustein für eine spezifische, in Kapitel 7 bestimmte, Komponente relevant ist.

ISMS: Sicherheitsmanagement

Tabelle 14: Relevanz der Bausteine aus der Schicht ISMS: Sicherheitsmanagement

ID	Baustein	Relevant?	Begründung (falls nicht relevant)
ISMS.1	Sicherheitsmanagement	Ja	

ORP: Organisation und Personal

Tabelle 15: Relevanz der Bausteine aus der 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 (Anforderungsmanagement)	Ja	

⁷ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (abgerufen am 18.05.2022)

CON: Konzeption und Vorgehensweise

Tabelle 16: Relevanz der Bausteine aus der Schicht CON: Konzeption und Vorgehensweise

ID	Baustein	Relevant?	Begründung (falls nicht relevant) und Hinweise
CON.1	Kryptokonzept	Ja	Abhängig von Satellitenmission, für Kontrolle des Satelliten aber erforderlich.
CON.2	Datenschutz	Nein	Es findet i.d.R. keine Verarbeitung von personenbezogenen oder -beziehbaren Daten statt
CON.3	Datensicherungskonzept	Ja	
CON.6	Löschen und Vernichten	Ja	
CON.7	Informationssicherheit auf Auslandsreisen	Ja	
CON.8	Software-Entwicklung	Ja	
CON.9	Informationsaustausch	Ja	
CON.10	Entwicklung von Webanwendungen	Nein	Es werden i.d.R. keine Webanwendungen entwickelt.

Unter Baustein CON.1 Kryptokonzept sollte eine adäquate Verschlüsselung der Kommunikation insbesondere der Satellitenkontrolle gefasst werden, um die Schutzziele Vertraulichkeit, Integrität und Authentizität der Kommunikation zu erreichen. Dazu sollten die zu schützenden Kommunikationsbeziehungen definiert und die relevanten Schutzziele (ggf. nur eine Auswahl obiger Schutzziele) zugeordnet werden. Für die Auswahl geeigneter Kryptoverfahren wird die Technische Richtlinie TR 02102 des BSI empfohlen.

OPS: Betrieb

Tabelle 17: Relevanz der Bausteine aus der Schicht OPS: Betrieb

ID	Baustein	Relevant?	Begründung (falls nicht relevant) und Hinweise
OPS.1.1.2	Ordnungsgemäße IT-Administration	Ja	
OPS.1.1.3	Patch- und Änderungsmanagement	Ja	Kann unterschiedlich gehandhabt werden zwischen Bodensegment und Satellit
OPS.1.1.4	Schutz vor Schadprogrammen	Ja	
OPS.1.1.5	Protokollierung	Ja	
OPS.1.1.6	Software-Tests und -Freigaben	Ja	
OPS.1.1.7	Systemmanagement	Ja	
OPS.1.2.2	Archivierung	Ja	Testdaten aus Simulationen sowie AIV/AIT sollten über die Missionsdauer archiviert werden, um übersehene Trends zu ggf. im Orbit auftretenden Fehlern recherchieren zu können.
OPS.1.2.4	Telearbeit	Ja	
OPS.1.2.5	Fernwartung	Ja	
OPS.2.1	Outsourcing für Kunden	Nein	
OPS.2.2	Cloud-Nutzung	Ja	

ID	Baustein	Relevant?	Begründung (falls nicht relevant) und Hinweise
OPS.3.1	Outsourcing für Dienstleister	Ja	

DER: Detektion und Reaktion

Tabelle 18: Relevanz der Bausteine aus der Schicht DER: Detektion und Reaktion

ID	Baustein	Relevant?
DER.1	Detektion von sicherheitsrelevanten Ereignissen	Ja
DER.2.1	Behandlung von Sicherheitsvorfällen	Ja
DER.2.2	Vorsorge für die IT-Forensik	Ja
DER.2.3	Bereinigung weitreichender Sicherheitsvorfälle	Ja
DER.3.1	Audits und Revisionen	Ja
DER.3.2	Revision auf Basis des Leitfadens IS-Revision	Ja
DER.4	Notfallmanagement	Ja

APP: Anwendungen

Tabelle 19: Relevanz der übergeordneten Bausteine aus der Schicht APP: Anwendungen

ID	Baustein	Relevant?
APP.7	Entwicklung von Individual-Software	Ja

Die ebenfalls für den gesamten Informationsverbund geltenden Bausteine SYS.3.2.2 Mobile Device Management (MDM) und IND.1 Prozessleit- und Automatisierungstechnik finden keine Anwendung.

8.2.2. Bausteine pro Zielobjekt

In den folgenden Tabellen werden die Systembausteine aufgeführt. Hier ist entscheidend, ob der Baustein für ein spezifisches, in Abschnitt 7 bestimmtes, Zielobjekt relevant ist.

APP: Anwendungen

Tabelle 20: Relevanz der Bausteine aus der Schicht APP: Anwendungen

ID	Baustein	Zielobjekte	Anmerkung
APP.1.1	Office-Produkte	A115	
APP.1.2	Web-Browser	A115	
APP.1.4	Mobile Anwendungen (Apps)	S115, S211, S214, S218, S219	
APP.2.1	Allgemeiner Verzeichnisdienst	A101	
APP.2.2	Active Directory	A101	
APP.2.3	OpenLDAP	A101	
APP.3.1	Webanwendungen und Webservices	A105	
APP.3.2	Webserver	A105	
APP.3.3	Fileserver	A106	
APP.3.4	Samba	-	Nicht im Einsatz.
APP.3.6	DNS-Server	A103	
APP.4.2	SAP-ERP-System	A212	

ID	Baustein	Zielobjekte	Anmerkung
APP.4.3	Relationale Datenbanksysteme	A212, S109, S201, S217	
APP.4.4	Kubernetes	S108	
APP.4.6	SAP ABAP-Programmierung	-	Nicht im Einsatz.
APP.5.2	Microsoft Exchange und Outlook	A114, A115	
APP.5.3	Allgemeiner E-Mail-Client und -Server	A114, A115	
APP.6	Allgemeine Software	A101, A102, A103, A104, A105, A106, A107, A108, A109, A110, A111, A114, A115, A201, A202, A203, A204, A205, A206, A207, A208, A209, A210, A211, A212, A213, A214, A215, A216, A217, A218, A219, A301, A302, A303, A304, A220, A305, A221, A306	

SYS: IT-Systeme

Tabelle 21: Relevanz der Bausteine aus der Schicht SYS: IT-Systeme

ID	Baustein	Zielobjekte	Anmerkung
SYS.1.1	Allgemeiner Server	S101, S102, S103, S104, S105, S106, S107, S108, S109, S111, S114, S115, S201, S202, S203, S204, S205, S206, S207, S208, S209, S210, S211, S212, S213, S214, S215, S216, S217, S218, S219, S301, S302, S303, S304, S220, S305, S221, S306	
SYS.1.2.2	Windows Server 2012	S101, S103, S104, S105, S106, S107, S108, S109, S111, S114, S201, S203, S205, S207, S209, S212, S217	
SYS.1.3	Server unter Linux und Unix	S101, S103, S104, S105, S106, S107, S108, S109, S111, S114, S201, S203, S205, S207, S209, S212, S217	
SYS.1.5	Virtualisierung	S107	
SYS 1.6	Containerisierung	S108	
SYS.1.7	IBM Z	-	Nicht im Einsatz.
SYS.1.8	Speicherlösungen	S102	
SYS.2.1	Allgemeiner Client	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
SYS.2.2.2	Clients unter Windows 8.1	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
SYS.2.2.3	Clients unter Windows 10	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
SYS.2.3	Clients unter Linux und Unix	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	

ID	Baustein	Zielobjekte	Anmerkung
SYS.2.4	Clients unter macOS	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
SYS.3.1	Laptops	S115, S202, S204, S206, S208, S210, S211, S213, S214, S215, S216, S218, S219, S220	
SYS.3.2.1	Allgemeine Smartphones und Tablets	A113, S115, S211, S214, S218, S219	
SYS.3.2.3	iOS (for Enterprise)	A113, S115, S211, S214, S218, S219	
SYS.3.2.4	Android	A113, S115, S211, S214, S218, S219	
SYS.3.3	Mobiltelefon	A113	
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	S112	
SYS.4.3	Eingebettete Systeme	S301, S302, S304, S306, S221, S306	
SYS.4.4	Allgemeines IoT-Gerät	-	Nicht im Einsatz.
SYS.4.5	Wechseldatenträger	-	Nicht für den Einsatz empfohlen.

IND: Industrielle IT

Die Bausteine aus der Schicht IND: Industrielle IT sind nicht im Einsatz.

NET: Netze und Kommunikation

Tabelle 22: Relevanz der Bausteine aus der Schicht NET: Netze und Kommunikation

ID	Baustein	Zielobjekte	Anmerkung
NET.1.1	Netzarchitektur und -design	NET	
NET.1.2	Netzmanagement	NET	
NET.2.1	WLAN-Betrieb	NET	
NET.2.2	WLAN-Nutzung	NET	
NET.3.1	Router und Switches	NET	
NET.3.2	Firewall	NET	
NET.3.3	VPN	NET	
NET.4.1	TK-Anlagen	S110	
NET.4.2	VoIP	S110	
NET.4.3	Faxgeräte und Faxserver	-	Nicht im Einsatz.

INF: Infrastruktur

Tabelle 23: Relevanz der Bausteine aus der Schicht INF: Infrastruktur

ID	Baustein	Zielobjekte	Anmerkung
INF.1	Allgemeines Gebäude	G01, G02, G03, G04, G05	
INF.2	Rechenzentrum sowie Serverraum	R02	

ID	Baustein	Zielobjekte	Anmerkung
INF.5	Raum sowie Schrank für technische Infrastruktur	-	Nicht im Einsatz.
INF.6	Datenträgerarchiv	-	Nicht im Einsatz.
INF.7	Büroarbeitsplatz	R01	
INF.8	Häuslicher Arbeitsplatz	R01	
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume	-	Nicht im Einsatz.
INF.11	Allgemeines Fahrzeug	G06	
INF.12	Verkabelung	G01, G02, G03, G04, G05	
INF.13	Technisches Gebäudemanagement	-	Nicht im Einsatz.
INF.14	Gebäudeautomatisierung	-	Nicht im Einsatz.

Einige für Satelliten spezifische Zielobjekte können mit den vorhandenen Bausteinen des IT-Grundschutz nicht hinreichend modelliert werden. Für solche Objekte, denen in obiger Tabelle kein Baustein zugewiesen ist (z.B. die Räume „Satellit“ oder „Launch-Halle“), sollte der Anwender des Profils (üblicherweise mithilfe einer Risikoanalyse) abwägen, wie bzw. ob hier über allgemein gefasste Bausteine (z.B. Allgemeines Gebäude) hinaus Maßnahmen getroffen werden sollten. Dazu sollten gemäß der IT-Grundschutz-Methodik Anforderungen abgeleitet werden, um das angestrebte Schutzniveau zu erreichen.

8.3 Anforderungen an Satelliten

In diesem Kapitel werden einige satellitenspezifische Anforderungen, die über den Grundschutz hinausgehen, dargestellt. Ihre Anwendung kann missionsspezifisch bewertet werden. Diese Anforderungen beziehen sich auf unterschiedliche Aspekte in den Lebenszyklen des Satelliten, welche sich in folgende Kategorien aufteilen:

- Allgemeine Anforderungen
- Transport
- Starteinrichtung
- In Orbit Phase
- Bodensegment
- Außerbetriebnahme

8.3.1. Allgemeine Anforderungen

Allgemeine Anforderungen sind die Anforderungen, welche sich in mehr als einem Bereich wiederfinden.

8.3.1.1 Schwachstellenscanning

Das Schwachstellenscanning dient dem Entdecken und Einschätzen von Schwachstellen, dies sollte in allen Bereichen durchgeführt werden. Die Art und der Umfang des Scannings orientiert sich am Gefahrenpotential des Satelliten und der Mission.

Schwachstellenscanning ist die ganzheitliche Betrachtung möglicher Sicherheitsmängel, dies umfasst u.a. Infrastruktur, Personal, Lieferketten und Penetrationstests.

8.3.1.2 Angriffssimulation

Die Simulation von (die Informationssicherheit betreffenden) Angriffen (z.B. Penetration Testing & Thread Simulationen) sollte in verschiedenen Teilabschnitten der Integration und der In Orbit Phase mit Berücksichtigung des Bodensegments durchgeführt werden. Bei besonders gefährdeten Missionen ist eine Angriffssimulation auf das Check-out System, den Transport, die Starteinrichtung sowie die Phase der Launch-Kampagne zusätzlich in Betracht zu ziehen.

8.3.1.3 Sicherheitsmanagement

Der Satellitenhersteller/-betreiber sollte von seinen Unterauftragnehmern und allen beteiligten Unternehmen ein Sicherheitsmanagement bzw. etablierte Sicherheitsstandards fordern und die Einhaltung der Regelwerke (via ISMS-Self-Assessment oder Audit) ggf. prüfen. Auch der Geltungsbereich des Sicherheitsstandards ist hier auf die relevanten Bereiche zu untersuchen.

8.3.1.4 Konzeption und Integration

Während der Konzeptions- und Integrationsphase sollten der Satellit und die am Satelliten angebrachten Systeme geschützt werden, sodass eine Manipulation durch Zugriff Unbefugter von außen ausgeschlossen werden kann.

Die an den Satelliten zum Datenaustausch angebrachten EGSE und MGSE Systeme sollten gegen Fremdzugriff, nach aktuellem Stand der Technik, geschützt werden. Dies verringert das Risiko, dass der Satellit durch Zugriff von extern beschädigt werden könnte.

Denkbare Schadeneintritte wären u.a. die Tiefenentladung der Batterien oder das Beschädigen oder Zerstören des Satelliten durch Zugriff auf die MGSE. Der Satellit könnte beispielsweise durch Zugriff auf die Steuerungskontroller der MGSE zum Umstürzen gebracht werden oder es könnten vorhandene Sprengbolzen ausgelöst werden.

Ein sicheres Netzwerk, hohe Zugangskontrollen sowie Sorgfalt bei der Übergabe von Arbeiten verringern maßgeblich das Risiko eines Schadeneintritts.

8.3.2. Anforderungen an den Transport

Der Transport von der Integrationshalle zu den Teststationen, zwischen verschiedenen Einrichtungen bis hin zur Starteinrichtung ist zu schützen. Dabei sollte der Termin, die Route, der Spediteur sowie beteiligtes Personal möglichst geheim gehalten werden. Das Personal sollte über die Geheimhaltung belehrt und verpflichtet werden.

Eine Trennung wichtiger Elemente des Satelliten beim Transport, soweit dies im entsprechenden Integrationszustand überhaupt noch möglich ist, sollte geprüft werden. Ferner sollte überprüft werden, ob für einzelne Bauteile oder den Transportbehälter die Auswahl geeigneter Tamper-Maßnahmen notwendig und sinnvoll ist.

8.3.3. Starteinrichtung

Vor der Vergabe des Auftrags des Satellitenstarts an die Starteinrichtung ist die Einhaltung von Sicherheitsstandards und Anforderungen sicherzustellen. Identifizierte Risiken sind transparent aufzuzeigen und gemäß der gültigen Risikomethode zu bewerten.

8.3.4. Schnittmenge In Orbit Phase und Bodensegment

Die Verbindung zwischen Bodensegment und Satellit sollte besonders geschützt werden. Dazu sollten Maßnahmen getroffen werden, die die Erfüllung der Schutzziele sicherstellen. Dabei sind Authentisierung und Authentifizierung, sowie der Einsatz sicherer kryptographischer Verfahren geeignete Mittel, um die Integrität der Kommunikation sicherzustellen.

Notfallpläne und Sicherheitsmechanismen zur Erkennung und Abwehr von Bedrohungen sollten im System implementiert sein. Bedrohungen könnten u.a. Störversuche, Cyber-Angriffe auf Satelliten und/oder Bodensegment, Übernahme, Zerstörung, etc. sein.

Das Einsetzen von Intrusion Detection sowie Intrusion Protection Systemen (IDS/IPS) und auch eine umfangreiche Aufzeichnung und Auswertung von Log-Dateien erhöht die Möglichkeit, Angriffe und Anomalitäten aufzudecken. Ein umfangreiches System-Monitoring und weitere Sicherheitsmechanismen sollten daher geeignet in den Systemen implementiert sein.

Sollten Angriffe oder Angriffsversuche sowie andere Anomalitäten erkannt werden, so ist ein Wechsel der Kommunikationsverschlüsselung und weitere Maßnahmen wie z.B. der Wechsel von Kryptohardware und -software, Algorithmen und Schlüsseln zu prüfen. Je nach Schwere und Schaden des Angriffs können – neben den zu veranlassenden Melde- und Informationsketten – weitere Sofortmaßnahmen notwendig werden.

Die etablierten Verfahren sollten dem Bedienpersonal bekannt sein, regelmäßige Notfallübungen sollten die Verfahrenssicherheit und den Prozess stetig verbessern.

8.3.4.1 In Orbit Phase

Veränderungen an Hardware und ggf. auch an Softwaresystemen sind nicht ohne weiteres möglich, daher sollten in der Implementierung der Einbau wichtiger Redundanzsysteme eingeplant werden und der Wechsel zwischen den Systemen getestet werden.

Werden für den Satelliten oder im Satelliten direkt Fremdinformationen verarbeitet, so sollte ein geeigneter Integritätsschutz für diese Informationen implementiert werden. Fremdinformationen sind alle Informationen, die von externen Quellen zur Verarbeitung benötigt und angefordert werden, z.B. bei der Nutzung von GPS-Zeitsignalen.

8.3.4.2 Bodensegment⁸

Das Bodensegment sollte als direkte Verbindung zum Satelliten entsprechend nach dem Stand der Technik abgesichert werden. Das beinhaltet die Infrastruktursicherheit und die Prozesskenntnis des Personals bei auftretenden Anomalien/Notfällen/Angriffen.

Daher sollten Notfallpläne in Hard- und Softcopy vorhanden sein. Regelmäßige Übungen zur Sicherstellung der Prozesskenntnisse sollten etabliert sein. Bei Systemausfällen sollte, sofern es die Bauweise des Satelliten zulässt, in einen „Safemode“ übergegangen werden, dieser muss geeignete Reaktionen auf den Ausfall oder Angriff zulassen.

So sind beispielsweise bei Kommunikationsverlust sichere und schnelle Maßnahmen zu ergreifen, die eine Wiederherstellung sicherstellen. Auch anschließende umfangreiche Systemtests nach Ausfällen sind zur Gewährleistung einer störungsfreien Wiederaufnahme des Betriebes durchzuführen.

8.3.5. Außerbetriebnahme

Hat der Satellit sein Missionsende erreicht und kann aufgrund verbrauchter Ressourcen oder ausgefallener Systeme nicht mehr genutzt werden, wird dieser außer Betrieb genommen. Die Größe und Flughöhe des Satelliten entscheiden i.d.R. über die Art der Außerbetriebnahme. Dabei kann der Satellit in eine Umlaufbahn gebracht werden, sodass er in der Atmosphäre verglüht und zerstört wird. Alternativ werden Satelliten in einen Friedhofsorbit gesteuert und verbleiben dort.

⁸ Das Bodensegment wird in diesem Profil nicht vollumfänglich betrachtet, sondern auf die Schnittstelle zum Satelliten fokussiert, siehe Kap. 7.2, entsprechend zielen auch die Anforderungen in diesem Abschnitt auf diese Schnittstelle ab.

Verglüht der Satellit, so werden alle Informationen unwiederbringlich zerstört. Geschieht dies in einem überwachbaren Zeitfenster, sollte der Satellit bis zum Verglühen noch überwacht werden. Ist der Satellit vollständig verglüht, sind keine weiteren Maßnahmen erforderlich.

Benötigt der Satellit mehrere Jahre bis er verglüht oder wird er in den Friedhofsorbit gesteuert, befinden sich dort noch immer Informationen und ggf. Kryptomaterial. Um einen Fremdzugriff auf die Informationen ausschließen zu können, sollte sichergestellt werden, dass alle Informationen, vor Verbringung, unwiederbringlich gelöscht werden.

Auch möglich ist der Schutz wichtiger Geräte durch Tamper-Maßnahmen, welche im Prozess der Außerbetriebnahme aktiviert werden, um dadurch Geräte und Informationen zu zerstören. Sollten Maßnahmen dieser Art eingesetzt werden, so sind diese so zu wählen, dass kein weiterer Weltraumschrott generiert wird.

9 Restrisiko

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. Ein Restrisiko bleibt immer bestehen. Durch die Zusammenarbeit mit anderen Organisationen können gegebenenfalls vertrauliche Informationen an Institutionen übertragen werden, auf deren Sicherheitsmanagement Hersteller und Betreiber von Satelliten nur beschränkt Einfluss nehmen können. Auch eigene Mitarbeiter können gegebenenfalls, trotz Dienstanweisungen und Schulungen, absichtlich oder unbewusst, solche Informationen an Unbefugte weitergeben. Ferner birgt auch der Bezug von Dienstleistungen Dritter ein Restrisiko.

Gezielte Angriffe auf die Informationstechnik von Einrichtungen jeglicher Art nehmen zu. Bekannt gewordene Sicherheitslücken in den Systemen werden immer schneller ausgenutzt. Eine rechtzeitige Behebung durch entsprechende Updates ist nicht immer möglich. Dies betrifft insbesondere Systeme, bei denen während der Entwicklung kein spezieller Fokus auf die Informationssicherheit gelegt wurde.

10 Anwendungshinweise

Im Falle des vorliegenden Grundschutz-Profils sollte der Schutzbedarf jedes Prozesses missionsspezifisch gründlich überprüft werden, da dieser bei den meisten Satellitenmissionen über den hier angenommenen Schutzbedarf der Kategorie „Normal“ hinausgehen kann und entsprechend höhere Anforderungen gestellt werden sollten. Das Profil dient lediglich als Schablone und muss individuell angepasst werden.

11 Checkliste – Mindestanforderungen für die IT-Sicherheit in Weltrauminfrastrukturen

Tabelle 24: Checkliste – Mindestanforderungen für die IT-Sicherheit in Weltrauminfrastrukturen

	Element	Notwendige Aktion	Berücksichtigt? Ja / Nein	Verantwortlich	Ggf. einzuleitende Maßnahmen	Datum
1	Räume / Gebäude					
1.1	Büro	Sicherheitsanforderungen identifiziert?				
1.2	Serverraum	Sicherheitsanforderungen identifiziert?				
1.3	Satellitenintegrationsraum/-halle	Sicherheitsanforderungen identifiziert?				
1.4	Testraum/halle	Sicherheitsanforderungen identifiziert?				
1.5	Transportcontainer	Sicherheitsanforderungen identifiziert?				
1.6	Launchhalle	Sicherheitsanforderungen identifiziert?				
1.7	Satellit	Sicherheitsanforderungen identifiziert?				
1.8	RZ-Raum Provider	Sicherheitsanforderungen identifiziert?				
1.9	Archiv	Sicherheitsanforderungen identifiziert?				
2	IT Infrastruktur					
2.1	Allgemeine IT-Infrastrukturen	Sicherheitsanforderungen identifiziert?				
2.2	Spezielle S/W (Modell-, Analyseinstrumente etc.)	Sicherheitsanforderungen identifiziert?				
2.3	Hardware & Softwareentwicklung	Sicherheitsanforderungen identifiziert?				
2.4	Testequipment	Sicherheitsanforderungen identifiziert?				
3	Personal					
3.1	Sicherheitsbelehrung	Durchgeführt?				
3.2	Sicherheitsüberprüfung (falls nötig)	Durchgeführt?				

	Element	Notwendige Aktion	Berücksichtigt? Ja / Nein	Verantwortlich	Ggf. einzuleitende Maßnahmen	Datum
3.3	Ausbildung / Training	Durchgeführt?				
4	Unterauftragnehmer (UAN)					
4.1	Wurde der UAN überprüft, ob er die geforderten Sicherheitsanforderungen erfüllen kann?	Durchgeführt?				
4.2	Beinhalten Ausschreibungen und Spezifikationen klare Sicherheitsanweisungen?	Durchgeführt?				
4.3	Wird die Einhaltung der Sicherheitsanforderungen regelmäßig überprüft?	Durchgeführt?				
4.4	Ist die Kommunikation zwischen Auftraggeber und UAN gegen Dritte abgesichert?					
4.5	externe Mitarbeiter					
4.5.1	Sicherheitsbelehrung	Durchgeführt?				
4.5.2	Sicherheitsüberprüfung (falls nötig)	Durchgeführt?				
4.5.3	Ausbildung / Training	Durchgeführt?				
4.5.4	Schnittstelle etablieren	Durchgeführt?				
5.	Integration und Zusammenbau aller Systemkomponenten incl. aller notwendigen Tests (AIT)					
5.1	Zugangskontrolle	Sicherheitsanforderungen identifiziert?				
5.2	Kontrolle der MA nach Beendigung der Arbeiten (ggf. täglich)	Durchgeführt?				
6	Transport					
6.1	Transportunternehmen	bekannt?				
6.2	Transportunternehmen	unbekannt?				
6.2.1	Sicherheitsüberprüfung durchgeführt?	Durchgeführt?				

	Element	Notwendige Aktion	Berücksichtigt? Ja / Nein	Verantwortlich	Ggf. einzuleitende Maßnahmen	Datum
	6.2.2 Sicherheitsbelehrung	Durchgeführt?				
	6.2.3 ggf. Training	Durchgeführt?				
	6.3 Container	Ausreichend gesichert				
	6.4 Begleitpersonal	Notwendig?				
	6.5.1 Falls ja, Sicherheitsbelehrung	Durchgeführt?				
	6.5.2 Falls ja, ggf. Training	Durchgeführt?				
7	Satellitenbetrieb					
	7.1 Kommunikation	abgesichert?				
	7.2 Datentransfer (Payload)	abgesichert?				
	7.3 Überwachung und Erkennung von Gefahren im Orbit	vorhanden?				
	7.3.1 Störung der Kommunikation	Berücksichtigt?				
	7.3.2 Blendung	Berücksichtigt?				
	7.3.3 Täuschung	Berücksichtigt?				
	7.3.4 Feindliche Übernahme	Berücksichtigt?				
	7.3.5 Feindliche Annäherung	Berücksichtigt?				
	7.3.6 Systemzerstörung (z.B. durch kinetische , Laser-, RF- Waffen oder Teilchenstromsysteme)	Berücksichtigt?				
	7.4 Notfallpläne	vorhanden?				
8	Außerbetriebnahme					
	8.1 Wurden sämtliche Bauteile beim Absturz zerstört	Status				
	8.2 Wurde der Satellit auf einen sicheren Friedhofsorbit verbracht	Status				