

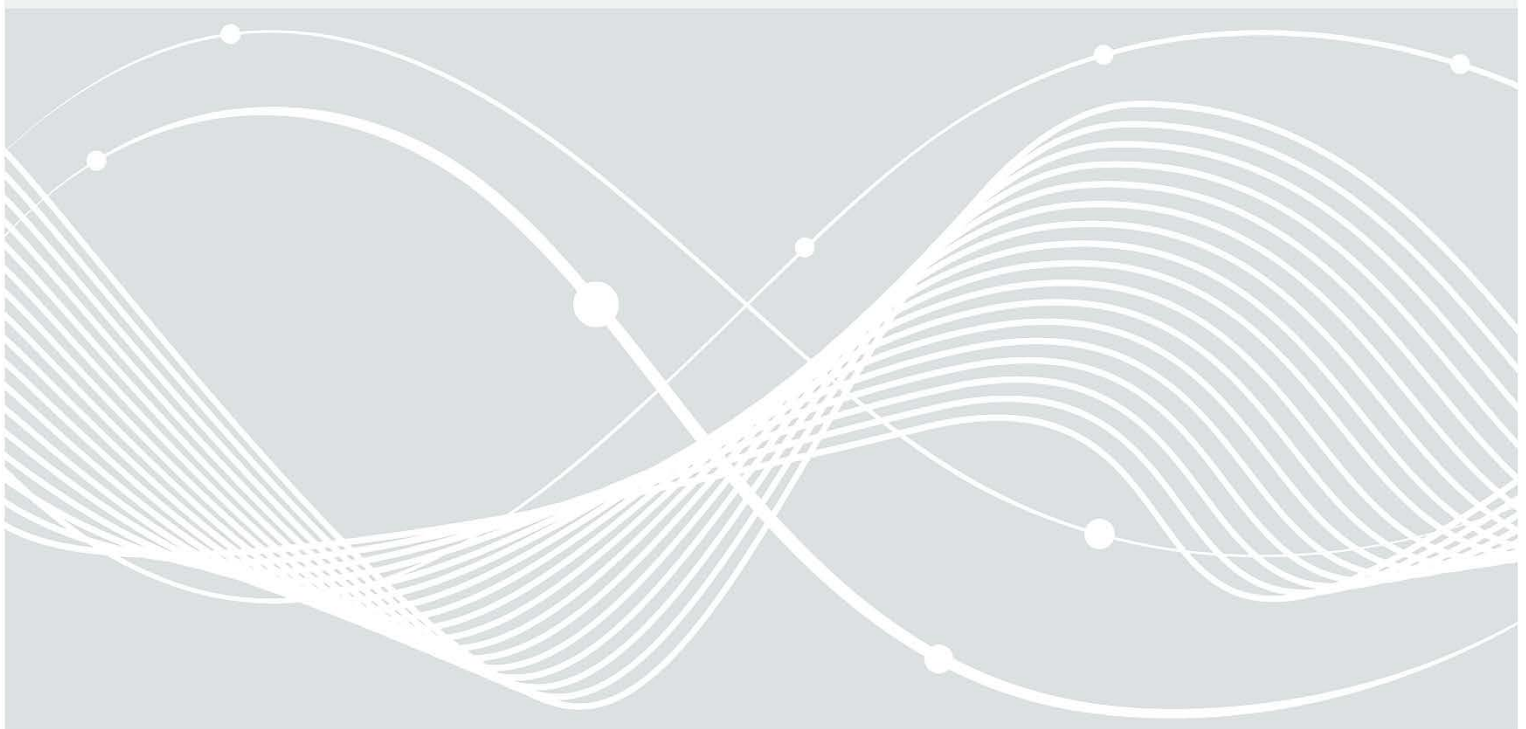


Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

IT-Grundschutz-Profil für Weltraumsysteme

Teil 2: Bodensegment - Mindestabsicherung über den gesamten Lebenszyklus



Änderungshistorie

Tabelle 1: Änderungshistorie

Version	Datum	Beschreibung
1.0	12.04.2024	Erstveröffentlichung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Internet: <https://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2024

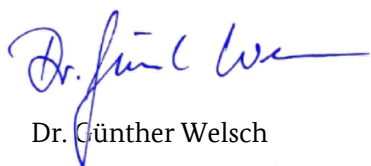
Vorwort der Abteilungsleitungen Krypto-Technik und Wirtschaft und Gesellschaft

Seit 2021 unterhält das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine aus verschiedenen Fachleuten der Wirtschaft, der Verwaltung und der Forschung bestehende Arbeitsgruppe, welche sich des Themas Cybersicherheit von Weltrauminfrastrukturen angenommen hat. Mittlerweile ist diese Arbeitsgruppe Teil des Expertenkreises „Cybersicherheit im Weltraum“ der Allianz für Cybersicherheit geworden.

Nach der Veröffentlichung des IT-Grundschutz-Profiles für Weltrauminfrastrukturen und der Technischen Richtlinie für Weltraumsysteme im Jahr 2022 hat sich der Expertenkreis nun des Themas Cybersicherheit des Bodensegments von Satellitenmissionen angenommen. Nahezu alle Satellitenmissionen – ob kommerziell, militärisch oder wissenschaftlich – nutzen unverzichtbar Bodensysteme für die Steuerung und Kontrolle der Satelliten. Mit zunehmender Anzahl von Satelliten und einem globalen Netz von Bodenstationen werden Satellitenmissionen auch für Cyber-Angriffe empfänglicher. Das Risiko eines erfolgreichen Cyberangriffs auf einen Satelliten, oder auch eine ganze Konstellation, wird damit größer und bedarf einer professionellen Behandlung möglicher Angriffsvektoren und der daraus resultierenden potentiellen Schäden, wenn die Bodensegmente mit in die Betrachtung genommen werden. Insbesondere unter dem Gesichtspunkt einer zunehmenden Kritikalität der Satellitenkommunikationsverbindungen für Wirtschaft und Industrie ist es folgerichtig, Bodenstationen als Teil einer Kritischen Infrastruktur mit einzubeziehen.

Mit dem hier vorgelegten IT-Grundschutz-Profil für das Bodensegment wird nun eine Reihe von Dokumenten fortgeschrieben, welche die Cyber-Sicherheit von Satelliten und ihren genutzten Infrastrukturen umfassend behandelt. Das vorliegende IT-Grundschutz-Profil für das Bodensegment ist, wie auch die anderen beiden Dokumente dieser Publikationsreihe, als Empfehlung und Handreichung zu verstehen. Es soll Raumfahrtakteuren bei der Erstellung und Umsetzung eines Informationssicherheitskonzeptes auf Basis der IT-Grundschutz Methodik unterstützen. Die einzelnen Schritte werden dabei beispielhaft anhand einer dargestellten Strukturanalyse durchgeführt. Das Ergebnis kann als Schablone genutzt werden, die für das eigene Bodensegment adaptiert werden und somit als Basis für ein Informationssicherheitskonzept dienen kann.

Wir danken allen Mitgliedern des Expertenkreises „Cybersicherheit im Weltraum“ für Ihr Engagement das vorliegende IT-Grundschutz-Profil in nun schon bewährter Qualität in gemeinsamer Arbeit mit dem BSI zu erstellen und auch zukünftig zu pflegen.



Dr. Günther Welsch

Leiter Abteilung Krypto-Technik



Dr. Timo Hauschild

Leiter Abteilung Wirtschaft und Gesellschaft

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik, ACS-Expertenkreis Cybersicherheit im Weltraum

Version:	1.0
Revisionszyklus:	2-jährlich
Version IT-Grundschutz-Kompendium	2023

Abkürzungsverzeichnis

Tabelle 2: Abkürzungsverzeichnis

Abkürzung	Bedeutung
AG	Auftraggeber
AN	Auftragnehmer
BCM	Business Continuity Management
BIA	Business Impact Analyse
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI Gesetz
CCSDS	Consultative Committee for Space Data Systems
COTS	Components/Commercial Off The Shelf
CRM	Customer Relationship Management
ECSS	European Cooperation for Space Standardization
EGNOS	European Geostationary Navigation Overlay Service
EGSE	Electrical Ground Support Equipment
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GP	Geschäftsprozess
GPS	Global Positioning System
IDE	Integrated Development Environment
ECSS	European Cooperation for Space Standardization
IoT	Internet of Things
ISL	Inter-Satellite-Link
ISMS	Information Security Management System
KRITIS	Kritische Infrastrukturen
LEO	Low Earth Orbit
LEOP	Launch and Early Operations/Orbit Phase
MCC	Mission Control Center
MCS	Mission Control System
MEO	Medium Earth Orbit
NEO	Near-Earth Objects
NIST	National Institute of Standards and Technology
OBSW	On Board Software
PNT	Position, Navigation and Timing
RMS	Risikomanagementsystem

Abkürzung	Bedeutung
RTO	Recovery Time Objective
SAT	Satellite
SATCOM	Satellite Communication
SCC	Satellite Control Center
SSA	Space Situational Awareness
SVT	System Validation Test
TM	Telemetry
TR	Technische Richtlinie
TTC	Telemetry, Tracking and Command
USV	Unterbrechungsfreie Stromversorgung
VS	Verschlussache

Begriffe

Tabelle 3: Liste der verwendeten Begriffe

Begriff	Beschreibung
Akteur (Actor)	Ein Akteur ist eine handelnde Person innerhalb eines Systems. Der Akteur interagiert mit anderen Akteuren und mit der Infrastruktur des Systems.
Angriff (Attack)	Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen.
Anwendung	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).
Beam-Forming	Eine Art des Funkfrequenzmanagements, bei dem ein Funksignal auf ein bestimmtes Empfangsgerät ausgerichtet wird.
Beam-Hopping	Beam-Hopping ist ein Konzept mit dem die Datenübertragung via Satellit flexibel an das variable Datenaufkommen in etwaigen Gebieten angepasst werden kann. Statt statisch einen bestimmten Bereich mit Daten zu versorgen, schaltet der Satellit dabei zwischen verschiedenen Ausleuchtzonen hin und her. Das Umschalten der Satelliten-Beams richtet sich nach einem Zeitplan, der die aktuell benötigten Datenraten in den verschiedenen Versorgungsgebieten berücksichtigt.
Bedrohung (Threat)	Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.
Bedrohungsakteur oder Angreifer (Threat Actor, Attacker)	Ein Akteur wird zum Bedrohungsakteur oder Angreifer, wenn Motivation, Rechtfertigung und Gelegenheit für negative Handlungen bestehen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.
Betreiber	Im Kontext dieses Dokuments bezieht sich dieser Begriff auf den operativen Betreiber eines Weltraumsystems.

Begriff	Beschreibung
Bewältigungsmaßnahme (Security Control, Countermeasure) und die Qualität deren Umsetzung	Bewältigungsmaßnahmen sind Sicherheitsmaßnahmen sehr ähnlich, jedoch beziehen sie sich nicht strikt auf die Steuerung von Sicherheitsanforderungen, sondern dienen der Risikobehandlung von Gefährdungen. Die Qualität der Umsetzung einer Bewältigungsmaßnahme kann durch ein gefordertes VS-Sicherheitsniveau vorgegeben sein. Eine Zugangsbeschränkung kann beispielsweise in folgenden Qualitäten umgesetzt werden: Drehkreuz, Tür, Mantrap, Wachpersonal, Wachhunde, Videoüberwachung, etc.
Gefährdung (Applied Threat)	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.
Geschäftsprozess	Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.
Infrastruktur	Eine Infrastruktur umfasst alle physikalischen und technischen Anlagen eines Systems.
IT-Infrastruktur	IT-Infrastrukturen sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Infrastrukturen sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.
IT-Sicherheit	IT-Sicherheit ist eine Unterdisziplin der Informationssicherheit und bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen reduziert sind.
IT-System	Ein IT-System umfasst eine IT-Infrastruktur sowie die Verfahren zu deren Einsatz, Überwachung, Kontrolle, Betrieb, Nutzung und Schutz.
(VS-)Kontrollzone	Kontrollzonen sind Bereiche, in denen VS bearbeitet werden, wenn der persönliche Gewahrsam nicht gewährleistet werden kann. Die Aufbewahrung von VS außerhalb von VS-Verwahrgeplätzen ist hier nicht zulässig. Kontrollzonen sind besondere Formen von Sicherheitsbereichen.
Manipulation (Tamper)	Eine nicht-autorisierte Aktion an einem System, um eine Veränderung von Daten und/oder des vorgesehenen Verhaltens zu bewirken.
Prozess	Prozesse beschreiben, wie die Komponenten eines Systems (Infrastruktur und Akteure) zusammenwirken sollen, damit das System seine Aufgaben erfüllt.

Begriff	Beschreibung
Risiko (Risk)	<p>Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt.</p> <p>Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.</p>
Risikobehandlung (Risk Treatment)	<p>Mit Risikobehandlung wird der Prozess bezeichnet, bei dem Maßnahmen ausgewählt und eingerichtet werden, die sich auf die Risiken auswirken. Das Ziel ist in der Regel, das Risiko einer Gefährdung zu senken, indem z.B. die Eintrittswahrscheinlichkeit oder der mögliche Schaden des unerwünschten Ereignisses durch geeignete Maßnahmen reduziert wird (siehe Bewältigungsmaßnahme).</p> <p>Die Risikobehandlung fällt typischerweise in eine der folgenden Gruppen:</p> <ul style="list-style-type: none"> • Risikovermeidung (Risk Prevention) • Risikominderung (Risk Reduction/Control) • Risikoakzeptanz (Risk Acceptance) • Risikotransfer (Risk Transfer)
Risikomanagement (Risk Management)	<p>Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren. Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein. Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus</p> <ul style="list-style-type: none"> • Identifikation von Risiken, • Einschätzung und Bewertung von Risiken, • Behandlung von Risiken, • Überwachung von Risiken und • Risikokommunikation.
Schwachstelle (Vulnerability)	<p>Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.</p>

Begriff	Beschreibung
Sicherheitsanforderung (Control)	<p>Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben. Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff „control“ verwendet.</p> <p>Der IT-Grundschutz unterscheidet zwischen Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegensprechen. Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.</p>
Sicherheitsbereich	<p>Sicherheitsbereiche sind Bereiche, zu denen nur bestimmte Personenkreise Zugang haben. Der Zugang ist durch technische und/oder organisatorische Maßnahmen zu beschränken, um den Aufenthalt von Mitarbeitern, aber auch von externen Dienstleistern und Besuchern zu regeln.</p> <p>Die Notwendigkeit kann sich z.B. aus Arbeitsschutzgründen („safety“) oder Informationssicherheitsgründen („security“) ergeben.</p> <p>Im Umgang mit VS sind besondere Formen von Sicherheitsbereichen gefordert, da explizite Sicherheitsanforderungen an die Qualität der Umsetzung bestehen.</p> <p>Aber auch ohne explizite VS-Anforderungen können Sicherheitsbereiche notwendig sein (z.B. zum Schutz von Geschäftsgeheimnissen / Intellectual Property).</p>
Sicherheitsmaßnahme (Safeguard, Security Measure, Measure)	<p>Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein.</p> <p>Sicherheitsmaßnahmen dienen zur Erfüllung von Sicherheitsanforderungen.</p>
(VS-)Sperrzone	<p>VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher dürfen außerhalb von VS-Verwahrtgelassen in VS-Sperrzonen (Räume, Gebäude, Gebäudeteile oder abgegrenzte Freilandzonen) bearbeitet und verwahrt werden.</p> <p>Sperrzonen sind besondere Formen von Sicherheitsbereichen mit höheren Zutrittsbeschränkungen und Sicherheitsmaßnahmen.</p>
Stakeholder	<p>Eine Person oder Gruppe, die ein berechtigtes Interesse am Verlauf oder Ergebnis eines Prozesses oder Projektes hat.</p>
System	<p>Ein System besteht aus verschiedenen Komponenten (Infrastruktur und Akteuren), die miteinander interagieren (gemäß Prozessen), um bestimmte Aufgaben zu erfüllen.</p>

Begriff	Beschreibung
VS-Verwahrgelass	VS-Verwahrgelasse sind besonders gesicherte Räume, Schränke oder sonstige Behältnisse zur Aufbewahrung von Verschlusssachen.
Weltrauminfrastruktur	Unter dem Begriff Weltrauminfrastrukturen werden alle terrestrischen und orbitalen Infrastrukturen (z.B. Satelliten, Kontrollzentren, Bodenstationen) zusammengefasst, die mit den verschiedenen funktionalen Phasen von Weltraumsystemen verbunden sind, wie Betrieb und Nutzung, Kontrolle, Herstellung und Aspekte des Schutzes. Der gesamte Lebenszyklus wird dabei betrachtet.
Weltraumsystem	Oberbegriff für sämtliche Komponenten von Satelliten- und Weltraumlagesystemen. Darunter fallen Weltrauminfrastrukturen selbst sowie die Verfahren zu deren Einsatz, Überwachung, Kontrolle, Betrieb, Nutzung und Schutz.

Inhalt

1	Einleitung	14
1.1	Ziel des Dokuments	14
1.2	Struktur des Dokuments	15
2	Formale Aspekte.....	16
3	Haftungsausschluss.....	17
4	Liste der Autorinnen und Autoren.....	18
5	Management Summary	19
5.1	Zielgruppe	19
5.2	Zielsetzung.....	19
5.3	Aufgabe der Leitungsebene.....	19
6	Festlegung des Geltungsbereichs	21
6.1	Zielgruppe	21
6.2	Beschreibung des Schutzbedarfs	21
6.3	IT-Grundschutz Vorgehensweise.....	21
6.4	Hinweis zu Kritischen Infrastrukturen im Sinne des BSIG und der Kritisverordnung.....	21
6.5	Kompatibilität zu anderen Standards	22
7	Abgrenzung des Informationsverbundes.....	23
7.1	Bestandteile des Informationsverbundes.....	23
7.2	Nicht berücksichtigte Teile	24
8	Strukturanalyse.....	26
8.1	Geschäftsprozesse.....	26
8.1.1	Allgemeine IT-Infrastruktur.....	28
8.1.2	Lebensphase 1: Konzeption und Design	28
8.1.3	Lebensphase 2: Herstellung.....	28
8.1.4	Lebensphase 3: Betriebsvorbereitung	28
8.1.5	Lebensphase 4: Betrieb	29
8.1.6	Lebensphase 5: Außerbetriebnahme	31
8.2	Anwendungen	31
8.3	IT-Systeme	31
8.4	Netze und Netzkomponenten	31
8.5	Gebäude und Räume.....	32
9	Modellierung.....	33
10	Spezifische Hinweise.....	34
10.1	Prozesslandschaft und Verantwortungen.....	34
10.2	Externe Dienstleistungen.....	34
10.3	Betriebskommunikation	35

10.4	Risikomanagement	35
10.5	Business Continuity Management	36
11	Missionsmerkmale	39
11.1	Missionstyp	39
11.2	Orbit	41
11.3	Konstellationsgröße	41
11.4	Stakeholder	42
11.5	Zweck	42
11.6	Infrastruktur	43
12	Schutzbedarfsfeststellung	44
12.1	Fallstudie 1: Cubesat	44
12.2	Fallstudie 2: GNSS	45
12.3	Fallstudie 3: Telekommunikationsdienste	45
13	Anwendungshinweise und Restrisiko	47

1 Einleitung

Weltraumgestützte Dienste haben sich zu einem unverzichtbaren Bestandteil der modernen Gesellschaft entwickelt. Sowohl die Nationale Sicherheitsstrategie als auch die Raumfahrtstrategie der Bundesregierung stellen heraus, dass Weltraumsysteme für Gesellschaft, Wirtschaft und Wissenschaft und für die Funktionsfähigkeit des Staates einschließlich Kritischer Infrastrukturen nicht mehr wegzudenken sind. Satellitengestützte Kommunikation, Erdbeobachtung, Positionsbestimmung, Navigation sowie die Verfügbarkeit hochpräziser Zeitsignale gewährleisten essenzielle Anwendungen des Alltags, u.a. im Bereich Gesundheit, Bevölkerungsschutz, Landwirtschaft oder Verkehr und tragen zu Erkenntnissen des Klimawandels und dessen Auswirkungen bei. Immer mehr Akteure werden in Zukunft in den Weltraum drängen und weitere Anwendungen werden von der Zuverlässigkeit der Daten, Informationen und Dienste abhängig sein. Die sich daraus ergebenden Möglichkeiten sind umfangreich, müssen aber mit sicherheitsrelevanten Überlegungen einhergehen.

Neben natürlichen Ursachen, wie z.B. Weltraumwetter und dem Risiko der unbeabsichtigten Kollision mit anderen Weltraumsystemen, besteht die Gefahr vorsätzlicher Handlungen, z.B. mit Anti-Satelliten Waffen. Mit der zunehmenden Digitalisierung und Vernetzung sowie der starken Zunahme nichtstaatlicher Akteure wächst zudem die Angriffsfläche und -wahrscheinlichkeit für Cyberangriffe gegen Weltraumsysteme.

Ein adäquater Schutz bedarf einer Betrachtung der gesamten Weltrauminfrastruktur, d.h. der verschiedenen Segmente in allen Lebensphasen. In Ergänzung zu dem „IT-Grundschutz-Profil für Weltrauminfrastrukturen – Mindestabsicherung für den Satelliten über den gesamten Lebenszyklus“¹ bietet das vorliegende IT-Grundschutz-Profil Hilfestellung zur Absicherung des Bodensegments.

Bodensegmente sind dabei denselben Bedrohungen und äußeren Einflüssen ausgesetzt, denen auch Kritische Infrastrukturen in anderen Sektoren unterliegen. Mit der Verbindung zum Satelliten bieten Bodensegmente eine Möglichkeit zur Störung oder Schädigung des Raumsegments. Die erforderliche Vernetzung und Erreichbarkeit macht sie zudem interessant für Angreifer und vulnerabel.

1.1 Ziel des Dokuments

Das Dokument dient als Anleitung für die strukturierte Erstellung eines Informationssicherheitskonzepts für Bodensegmente. Ziel ist es, bei Anwendung des Dokuments auf Basis der IT-Grundschutz Methodik die Informationssicherheit für Bodensegmente zum Schutz von Vertraulichkeit, Verfügbarkeit und Integrität zu erhöhen. Das Bodensegment ist hier als ein Gesamtsystem zu verstehen, welches das Betriebsbodensegment bzw. Mission Control Center (MCC), das Satellitenkontrollzentrum bzw. Satellite Control Center (SCC) und die Telemetry Tracking and Command (TTC) Bodenstationen umfasst. Es werden lediglich die Schnittstellen zum Raumsegment (inkl. Link Segment) und Nutzersegment betrachtet (siehe Kapitel 7), die Funkstrecken selbst sind nicht Gegenstand dieses Dokuments.

Anhand eines exemplarischen Bodensegments werden über den gesamten Lebenszyklus hinweg die verschiedenen Schritte zur Erstellung einer Sicherheitskonzeption durchgespielt und Maßnahmen abgeleitet.

Der Begriff Informationssicherheit umfasst dabei den gesamten Bereich des Schutzes von Informationen und schließt, neben der IT-Sicherheit, auch organisatorische, personelle und umweltspezifische Rahmenbedingungen mit ein.

Anleitung, Hinweise und Erläuterungen sind allgemein gehalten, sodass das Dokument bei möglichst vielen Projekten angewendet werden kann. Folglich muss der Anwender bei der Erstellung des Sicherheitskonzepts entsprechend den Merkmalen und Eigenschaften des zugrundeliegenden

¹ Als Onlinedokument unter:

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html (Stand: 09.02.2024)

Bodensegments diese ergänzen und vertiefen. Beispielsweise müssen die zur Erfüllung der Schutzziele beschriebenen Maßnahmen je nach Bodensegment individuell angepasst und je nach Kritikalität ggf. noch ergänzt werden.

1.2 Struktur des Dokuments

Im Rahmen des IT-Grundschutz-Profils wurden in Kapitel 8.1 sechs Lebensphasen - angelehnt an den Lebenszyklus eines Bodensegments - identifiziert und betrachtet.

Ausgehend von diesen sechs Lebensphasen umfasst das vorliegende IT-Grundschutz-Profil für das Bodensegment:

- eine Liste relevanter Zielobjekte (Anwendungen, IT-Systeme und Gebäude/Räumlichkeiten), die es zu schützen gilt,
- eine Zuordnung der dazu passenden IT-Grundschutz-Bausteine mit Anforderungen und Umsetzungshinweisen, sowie
- allgemeine Anforderungen, die aufgrund weltraumspezifischer Prozesse über den Grundschutz hinausgehen.

Kapitel 5 fasst die Inhalte dieses Dokuments zusammen und beschreibt Zielgruppe und Aufgaben der Leitungsebene. Kapitel 6 erläutert den Geltungsbereich des IT-Grundschutz Profils. In Kapitel 7 wird der Muster-Informationsverbund definiert und abgegrenzt. Kapitel 8 stellt eine exemplarische Strukturanalyse mit Berücksichtigung der verschiedenen Lebensphasen dar. Zusätzlich werden in diesem Kapitel Annahmen, Erläuterungen und Abweichungen beschrieben.

Die Modellierung und Zuordnung relevanter BSI-IT-Grundschutz Bausteine sind im Kapitel 9 erfasst und beschrieben.

Kapitel 10 beschreibt für das Bodensegment spezifische Hinweise und Erfahrungen der Hersteller und Betreiber. Dies umfasst unter anderem eine Betrachtung von Prozessen, Verantwortlichkeiten und den Besonderheiten für das Bodensegment.

Kapitel 11 dient zur Erläuterung verschiedener Missionsmerkmale wie Orbit, Konstellationsgröße, Stakeholder, Zweck und Infrastruktur und wie diese sich auf den Schutzbedarf einer Mission auswirken können. Die Festlegung des Schutzbedarfs wird exemplarisch in Kapitel 12 beschrieben.

2 Formale Aspekte

Tabelle 4: Formale Aspekte

Aspekt	Beschreibung
Titel:	IT-Grundschutz-Profil für Bodensegmente – Mindestabsicherung für Bodensegment über den gesamten Lebenszyklus
Autorenschaft:	Siehe Kap. 3 „Liste der Autorinnen und Autoren“
Herausgeberschaft:	Bundesamt für Sicherheit in der Informationstechnik, Expertenkreis Cybersicherheit im Weltraum der Allianz für Cybersicherheit
Versionsstand:	1.0
IT-Grundschutz-Kompendium	Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2023.
Revisionszyklus:	Die Aktualität des Dokuments soll 2-jährlich überprüft werden.
Vertraulichkeit:	Das Dokument in der hier vorliegenden Version ist offen zugänglich.

3 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, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

4 Liste der Autorinnen und Autoren

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

Tabelle 5: Liste der Autorinnen und Autoren.

<i>Name</i>	<i>Organisation</i>
Dr. Johanna Niecknig	Bundesamt für Sicherheit in der Informationstechnik
Wendel Lohmer	Bundesamt für Sicherheit in der Informationstechnik
Rabea Harnisch	Bundesamt für Sicherheit in der Informationstechnik
Stefanie Grundner	Panaglobo GbR
Manuel Hoffmann	Thales Deutschland GmbH
André Penzien	Rheinmetall Eletronics GmbH
Maximilian Roth	Airbus Defence and Space GmbH
Tarsicio López Delgado	Rivada Space Networks GmbH
Frank Keck	secunet Security Networks AG
Sascha Fankhänel	Jade Hochschule Wilhelmshaven
Andreas Ebhardt	DLR GfR mbH; Spaceopal GmbH
Christoph Möbius	CGI Deutschland B.V. & Co. KG
Dr. Björn Appel	INFODAS GmbH
Justus Bach	INFODAS GmbH
Dr. Daniel Grötsch	INFODAS GmbH
Niels Lerch	INFODAS GmbH
Dr. André Kubelka-Lange	OHB Digital Connect GmbH
Sarah Hennig	OHB Digital Connect GmbH

Für die fachliche Qualitätssicherung wurde das Dokument geprüft durch:

Tabelle 6: Liste der weiteren Beteiligten an der Erstellung des IT-Grundschutz-Profils

<i>Name</i>	<i>Organisation</i>
Stefan Langhammer	OHB Digital Connect GmbH
Wim Fleischhauer	Rheinmetall Electronics
Jens Ender	CGI Deutschland B.V. & Co. KG
Karel Kotarowski	Airbus Defence and Space GmbH

5 Management Summary

5.1 Zielgruppe

Das IT-Grundschatz-Profil für Bodensegmente richtet sich an die Verantwortlichen für die Informationssicherheit im Bodensegment. Dies umfasst die Herstellung, einschließlich der Zuliefernden und Dienstleistenden, den Betrieb bis zur Außerbetriebnahme am Ende des Lebenszyklus der Mission (siehe Kapitel 6.1).

5.2 Zielsetzung

Dieses IT-Grundschatz-Profil für das Bodensegment soll den Anwendenden helfen, Informationssicherheit in allen Lebensphasen zu gewährleisten und an die missionsspezifischen Bedürfnisse anzupassen zu können. Es soll als Schablone dienen, den IT-Grundschatz des BSI in geeigneter Weise zu implementieren.

Dieses IT-Grundschatz-Profil definiert ein empfohlenes Vorgehen zum Nachweis der Absicherung, gemäß des festgelegten Schutzbedarfs für die Informationssicherheit des Bodensegments, das während aller Lebensphasen des Bodensegments berücksichtigt werden sollte. Dazu werden Geschäftsprozesse (GP), die sich an den Lebensphasen des Bodensegments orientieren, definiert. Entsprechend der Herangehensweise der Standard-Absicherung nach IT-Grundschatz werden Sicherheitsanforderungen, die erfüllt werden sollten, beschrieben. Die untersuchten Lebensphasen und deren GP sind:

- Lebensphase 0: Allgemeine IT-Infrastruktur,
- Lebensphase 1: Konzeption und Design,
- Lebensphase 2: Herstellung,
- Lebensphase 3: Betriebsvorbereitung,
- Lebensphase 4: Betrieb,
- Lebensphase 5: Außerbetriebnahme.

Dabei soll die Lebensphase 0 „Allgemeine IT-Infrastruktur“, die eingesetzte IT-Infrastrukturen umfassen, die in allen oben genannten Prozessen verwendet werden. Dieser Querschnittsprozess vereinfacht die Anwendung des IT-Grundschatzes innerhalb des IT-Grundschatz-Profils.

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

Bei den meisten Bodensegmenten wird ein höherer Schutzbedarf zugrunde zu legen sein, der die Anwendung von Anforderungen über die hier beschriebene Standard-Absicherung hinaus notwendig macht. Gleichmaßen kann es in Einzelfällen vorkommen, dass Anwendende des Profils entscheiden, gewisse Maßnahmen nicht umzusetzen. Diese Entscheidungen sollten durch eine Risikobetrachtung unterlegt und dokumentiert sein.

5.3 Aufgabe der Leitungsebene

Die Autorinnen und Autoren empfehlen der Leitungsebene von Einrichtungen im Bodensegment die Anwendung dieses IT-Grundschatz-Profils als Grundlage für das Informationssicherheitskonzept. Diese Empfehlung gilt für alle Lebensphasen der Strukturanalyse.

Die Autorinnen und Autoren weisen zudem auf eine angemessene Berücksichtigung und Handhabung von Informationssicherheitsrisiken in der Lieferkette hin. Daher ist durch die Leitungsebene dafür Sorge zu tragen, dass neben der für den Schutzbedarf notwendigen Absicherung nach IT-Grundschatz der Lieferkette, die Zuliefernden angemessen nach deren Vertrauenswürdigkeit ausgewählt werden. Im Falle

von Outsourcing von IT oder Prozessen empfehlen die Autorinnen und Autoren, die entsprechenden Dienstleistenden vertraglich zu verpflichten, eine Absicherung gemäß des festgelegten Schutzbedarfes (z.B. auf Grundlage dieses IT-Grundschutz-Profiles) nachzuweisen.

6 Festlegung des Geltungsbereichs

6.1 Zielgruppe

Das IT-Grundschutz-Profil für Bodensegmente richtet sich an die für die Informationssicherheit, die Informationstechnik sowie die Infrastruktursicherheit verantwortlichen Entscheidungsträger und Projektleiter. Der Anwendungsbereich ist in diesem Dokument das gesamte Bodensegment. Hersteller und Lieferanten in der Lieferkette können dieses Dokument anwenden.

6.2 Beschreibung des Schutzbedarfs

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

Da es sich bei dem vorliegenden IT-Grundschutz-Profil um Empfehlungen einer Mindestabsicherung handelt, die für möglichst viele Missionen im Bodensegment anwendbar sein soll, wurde in einer exemplarischen Schutzbedarfsanalyse die Modellierung von Fallbetrachtungen definiert. In diesem Zusammenhang werden drei unterschiedliche Fallbeispiele mit unterschiedlichen Schutzbedarfen betrachtet.

Für das vorliegende IT-Grundschutz-Profil wird daher der Schutzbedarf „Normal“ für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit als Mindest-Schutzbedarfsniveau festgelegt. Dargestellt wird diesbezüglich mindestens eine Standard-Absicherung der IT-Grundschutz-Vorgehensweise.

6.3 IT-Grundschutz Vorgehensweise

Der IT-Grundschutz des BSI bietet die Vorgehensweisen für 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 der Standardabsicherung des BSI-Standards 200-2. Sie hat einen umfassenden Schutz für alle Prozesse und Bereiche der Institution als Ziel und kann ebenfalls als Basis für ein höheres Schutzniveau dienen. Da für jedes Bodensegment der Schutzbedarf individuell festzustellen ist, wird empfohlen, an die Mission angepasst, einzelne Anforderungen aus dem erhöhten Schutzbedarf ebenfalls mit umzusetzen.

6.4 Hinweis zu Kritischen Infrastrukturen im Sinne des BSIG und der Kritisverordnung

Das vorliegende IT-Grundschutz-Profil kann zur Erfüllung der gesetzlichen Anforderungen an Betreiber Kritischer Infrastrukturen nach dem BSIG herangezogen werden. „Kritische Infrastrukturen (KRITIS)“ nach §§1-7 BSI-Kritisverordnung, sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. In der BSI-Kritisverordnung werden einzelne Sektoren näher betrachtet und darüber hinaus Schwellenwerte zur Bestimmung von Betreibern Kritischen Infrastrukturen aufgeführt. Darunter fallen u. a. Betreiber von Bodenstationen eines Satellitennavigationssystems.²

² Vgl. Anhang 7 Teil 3 Spalte A Nr. 1.7.2 „Bodenstation eines Satellitennavigationssystems“ BSI-KritisV, sowie Artikel 28 der Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates vom 11.12.2013 betreffend den Aufbau und Betrieb der europäischen Satellitennavigationssysteme und zur Aufhebung der Verordnung (EG) Nr. 876/2002 des Rates und der Verordnung (EG) Nr. 683/2008 des Europäischen Parlaments und des Rates.

Betreiber Kritischer Infrastrukturen sind nach §8a Abs. 1 BSIG verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Anforderungen an die Informationssicherheit können durch Evaluierung und Implementierung der Standardabsicherung des BSI-Standards 200-2, wie in Kapitel 6.3 beschrieben, erfüllt werden. Dabei muss überprüft werden, ob alle Komponenten, Systeme oder Prozesse hinreichend berücksichtigt sind.

Dieses IT-Grundschutz-Profil bietet Anwendern die Möglichkeit den ebenfalls nach §8a Abs. 1 BSIG geforderten Stand der Technik für zu treffende Maßnahmen mit Hilfe der BSI IT-Grundschutzmethodik für den individuellen Anwendungsbereich zu konkretisieren.

Weitere Anforderungen an Betreiber Kritischer Infrastrukturen, die gegebenenfalls über die Empfehlungen dieses IT-Grundschutz-Profiles hinaus gehen, sind in den entsprechenden Orientierungshilfen³ beschrieben und müssen zur gesetzlichen Pflichterfüllung angewendet werden.

6.5 Kompatibilität zu anderen Standards

Durch eine Umsetzung der Standard-Absicherung besteht Kompatibilität zur ISO-Norm 27001. 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.

Darüber hinaus ist zu prüfen, ob gesetzliche Vorgaben, wie z.B. bei der Hersteller- und Lieferantenauswahl durch Export-/Import-Richtlinien, zu berücksichtigen sind. Bei KRITIS-relevanten Missionen sind u.U. zusätzlich gesetzliche Lieferkettenanforderungen zu erfüllen.

³ OH Nachweise: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-nachweise.html?nn=126476> (Stand: 09.02.2024)

OH B3S: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-b3s.pdf?__blob=publicationFile&v=5 (Stand: 09.02.2024)

OH SzA: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=15 (Stand: 09.02.2024)

7 Abgrenzung des Informationsverbundes

7.1 Bestandteile des Informationsverbundes

Dieses IT-Grundschutz-Profil betrachtet das Bodensegment eines Weltraumsystems. Die Einordnung in das Gesamtsystem zeigt Abbildung 1. Bei der Betrachtung des Bodensegments und der Identifizierung dessen Prozesse wird die grundsätzliche Unterteilung der Satelliten in Plattform und Nutzlast berücksichtigt.

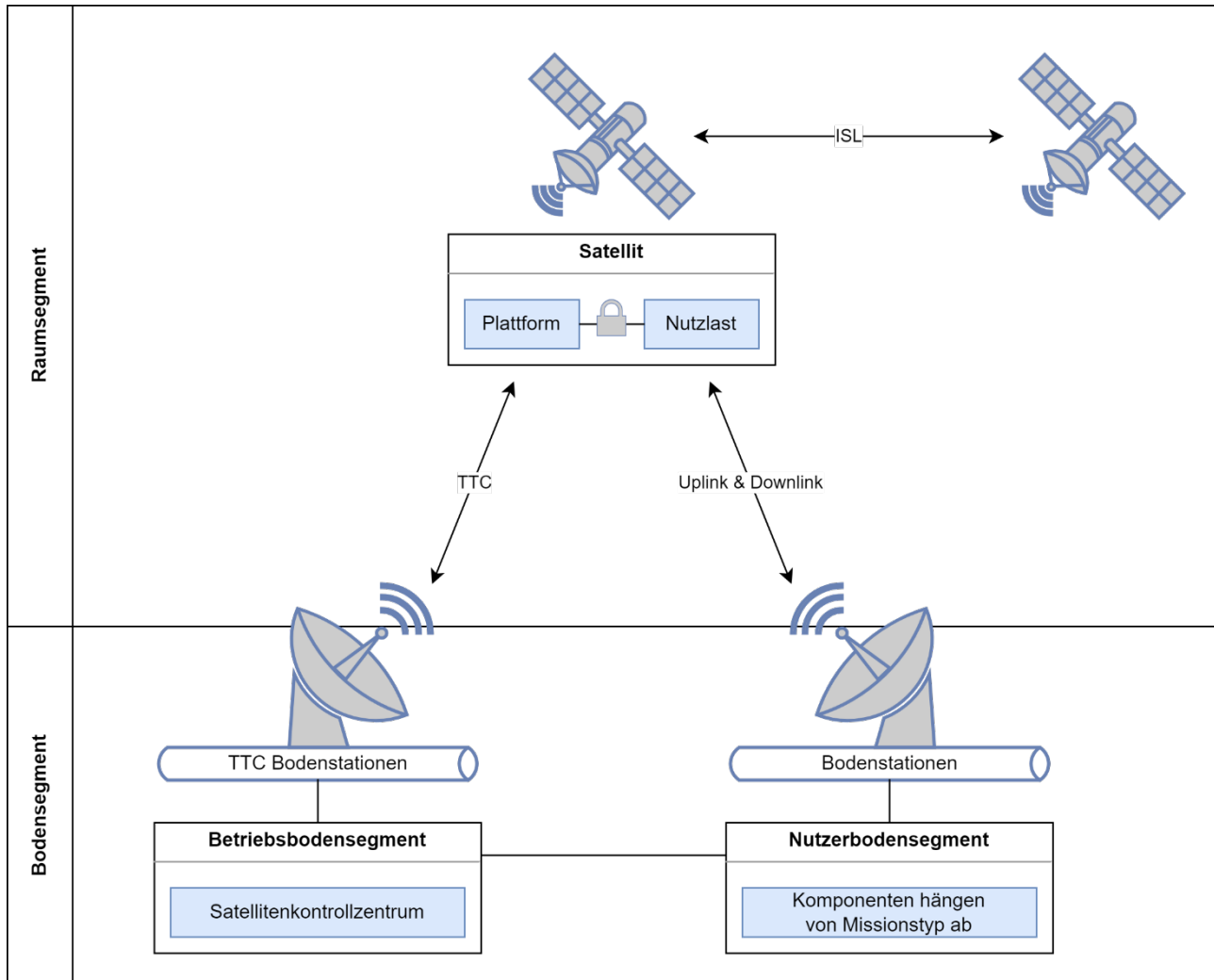


Abbildung 1: Systemgrenzen und Übergänge

Der Fokus dieses IT-Grundschutz-Profiles liegt auf dem Bodensegment als Informationsverbund selbst, das umfasst Kontrollzentren, Bodenstationen, Supportinfrastrukturen und Netzwerke. Zum Informationsverbund Bodensegment gehören im Allgemeinen alle Prozesse und Verfahren, die während des gesamten Lebenszyklus direkt oder über prozessuale Schnittstellen relevant sind, sowie alle technischen Bestandteile wie Anwendungen, IT-Systeme, Räume und Gebäude, die diese Prozesse und Verfahren unterstützen.

Das Bodensegment, als Informationsverbund im IT-Grundschutz-Profil, lässt sich in folgende Hauptkomponenten untergliedern:

Betriebsbodensegment (Operations Ground Segment)

Im Betriebsbodensegment laufen alle Prozesse ab, um die Kommandierung der Satelliten und somit einen unterbrechungsfreien und sicheren Betrieb des Satelliten zu gewährleisten. Damit werden ebenfalls der Betrieb der Nutzlasten und die eigentliche Ausführung der Missionsaufgaben ermöglicht.

Typische Komponenten im Betriebsbodensegment sind Satellitenkontrollzentren und TTC-Bodenstationen, welche durch Netzwerke verbunden sind.

TTC sind die für die Satellitenkontrolle notwendigen Operationen der Bodenstation:

- *Telemetry* für die am Betriebsbodensegment empfangenen Daten (Downlink),
- *Command* für die vom Betriebsbodensegment gesendeten Daten (Uplink) und
- *Tracking* für die Bahnverfolgung eines Satelliten und Entfernungsmessung über spezielle Sensorik einer TTC-Bodenstation, z.B. Radar oder Funkpeilung. Das Tracking ist eine der besonderen Funktionen, welche die TTC-Bodenstation von einer normalen Bodenstation (nur Downlink, ggf. auch Uplink) unterscheidet.

Ziel der TTC-Kommunikation ist eine sichere Verbindung zwischen dem Satellitenkontrollzentrum und der Plattform des Satelliten. Aufgrund ihres Ende-zu-Ende-Charakters ist die sichere TTC-Kommunikation ein Element, welches sowohl in dem vorliegenden IT-Grundschatz-Profil, als auch im IT-Grundschatz-Profil und in der Technischen Richtlinie (TR) des Raumsegments betrachtet wird.

Nutzerbodensegment (User Ground Segment)

Die Komponenten und Prozesse im Nutzerbodensegment sind stark vom Missionstyp des Weltraumsystems abhängig. Kommunikation mit der Nutzlast über Bodenstationen; diese Kommunikation mit der Nutzlast kann (je nach Systemkonzept) auch als Service des Betriebsbodensegments über die TTC-Kommunikation realisiert werden.

- Konfiguration/Administration der Nutzlast
- Verarbeitung und Bereitstellung von empfangenen Nutzlastdaten
- Bereitstellung und Uplink von Nutzlastdaten zum Satelliten
- Die zu betrachtenden Prozesse werden durch den Nutzlastbetreiber durchgeführt. Davon unabhängig ist die Konfiguration und Nutzung der Nutzlast und/oder mit den Nutzlastdaten. Der Nutzlastbetreiber muss dabei nicht zwingend identisch mit dem Betreiber des Betriebssegments sein.

7.2 Nicht berücksichtigte Teile

Sämtliche Elemente des Raumsegments werden im IT-Grundschatz-Profil für Weltrauminfrastrukturen behandelt und sind dementsprechend nicht Teil des Informationsverbundes im vorliegenden IT-Grundschatz-Profil. Die Kommunikationsverbindungen zwischen Raum- und Bodensegment wurden dabei ebenfalls dem Raumsegment zugeordnet, sodass sich als Schnittstelle zwischen Raum- und Bodensegment die Antennen der Bodenstationen ergeben. Die Kommunikation zwischen Satelliten (Inter-Satellite-Link (ISL)) ist in dieser Betrachtung ebenfalls dem Raumsegment zugeordnet.

Darüber hinaus wurden das Nutzerbodensegment sowie zugehörige Prozesse nicht berücksichtigt, um eine scharfe und sinnvolle Abgrenzung des Dokuments zu erlauben. Die Grundschatz Methodik im Allgemeinen und die gewonnenen Erkenntnisse aus dem vorliegenden IT-Grundschatz-Profil lassen sich durch den Anwender aber entsprechend übertragen, um ein gesamtheitliches Schutzkonzept umzusetzen.

Nicht im Betrachtungsumfang sind somit konkret:

- Satellit und die zugeordneten Entwicklungs-, Test- und Startprozesse am Boden,
- Schnittstellen des Betriebsbodensegments zu externen Dienstleistern (z.B. Space Situational Awareness, SSA),
- Im Nutzerbodensegment:
 - Kommunikation mit der Nutzlast,
 - Verarbeitung von empfangenen Nutzlastdaten,

- Kundenmanagement, Nutzeradministration und ähnliche Dienste.

Der Hersteller/Betreiber eines Bodensegments ist jedoch angehalten, darauf zu achten, dass auch in diesen Systemen ein vergleichbares Sicherheitsniveau durch dessen Betreiber nachgewiesen werden kann.

8 Strukturanalyse

Die Strukturanalyse legt fest, welche Objekte und Anwendungen, IT-Systeme und Infrastrukturen für die wesentlichen Prozesse im Lebenszyklus eines Bodensegments relevant sind und im Sinne des IT-Grundschutzes abgesichert werden müssen. Damit bietet sie eine Arbeitsgrundlage für dieses Profil.

Die im Annex dargestellte Strukturanalyse bildet ein exemplarisches Bodensegment ab und muss an die tatsächlichen Projekte angepasst werden. Hierfür muss die Strukturanalyse auf korrelierende Systeme und Anwendungen geprüft, sowie ggf. angepasst werden.

In diesem Profil umfasst die Strukturanalyse die unterschiedlichen Lebensphasen des Bodensegments von der Konzeption bis zur Außerbetriebnahme. Innerhalb dieser Lebensphasen erfolgt die Zuordnung zu entsprechenden GP, um anschließend die erforderlichen Anwendungen und IT-Systeme präzise zu definieren.

Die IT-Systeme samt ihrer Anwendungen können in unterschiedlichen Gebäuden und Räumlichkeiten untergebracht sein. Es ist erforderlich, diese Standorte in Verbindung mit weiteren infrastrukturellen Anforderungen in Betracht zu ziehen und angemessen zu berücksichtigen.

Sind die Gegenstände der Strukturanalyse vollständig erfasst, können die in diesem Profil empfohlenen Grundschutzbausteine ausgewählt werden. Anhand der Auswahl werden die Anforderungen erfasst und die notwendigen Maßnahmen abgeleitet. Werden IT-Systeme und Anwendungen identifiziert, welche nicht in der Strukturanalyse des Profils berücksichtigt werden, müssen die entsprechenden Grundschutzbausteine aus dem IT-Grundschutz Kompendium in der Strukturanalyse des tatsächlichen Projekts ergänzt werden.

Weicht der zu schützende Informationsverbund von der hier dargestellten Strukturanalyse ab, sollten die zusätzlichen oder nicht vorhandenen Objekte dokumentiert und eine Nicht-Betrachtung begründet werden. Der Grundschutz-Methodik folgend, müssen Objekte den relevanten Komponenten des IT-Grundschutz Kompendiums zugeordnet werden. Die abgeleiteten Anforderungen sollten an den jeweiligen Schutzbedarf angepasst werden.

8.1 Geschäftsprozesse

Die identifizierten GP beschreiben die notwendigen Funktionen, die ein Bodensegment über die Lebenszeit eines Weltraumsystems hinweg erfüllen muss, um einen sicheren Betrieb des Systems gewährleisten zu können.

Die Lebensphasen - unterteilt in GP - beschreiben einen typischen Lebenszyklus eines Bodensegmentes und orientieren sich an dem BSI-Profil für Weltrauminfrastrukturen. Die Betrachtung der Lebensphasen gewährleistet eine zeitnahe und einheitliche Betrachtung der GP für spätere Lebenszyklen. In den GP gibt es Bereiche, die eine Abstimmung zwischen Auftragnehmer (AN), Auftraggeber (AG) und Betreiber erforderlich machen.

Eine Darstellung der GP aus der Strukturanalyse und der logische Zusammenhang für das Bodensegment ist in Abbildung 2 zu sehen. Der Satellitenbetrieb unterscheidet dabei zwischen Kontrolle bzw. Steuerung für die Satelliten-Plattform und der Satelliten-Payload. Die Satelliten-Plattform wird durch das Satellite Control Center (SCC) kontrolliert und gesteuert. Aus der Sicherheitsbetrachtung sind das SCC und die Satelliten-Plattform als die kritischsten Systeme anzusehen und werden daher rot gekennzeichnet. Für die Steuerung und Kontrolle der Satelliten-Payload ist dagegen das Mission Control Center (MCC) verantwortlich (grün gekennzeichnet). Das MCC kann bei Bedarf ausschließlich durch das SCC Änderungen an der Satelliten-Plattform, in Form von Änderungsanfragen, vornehmen.

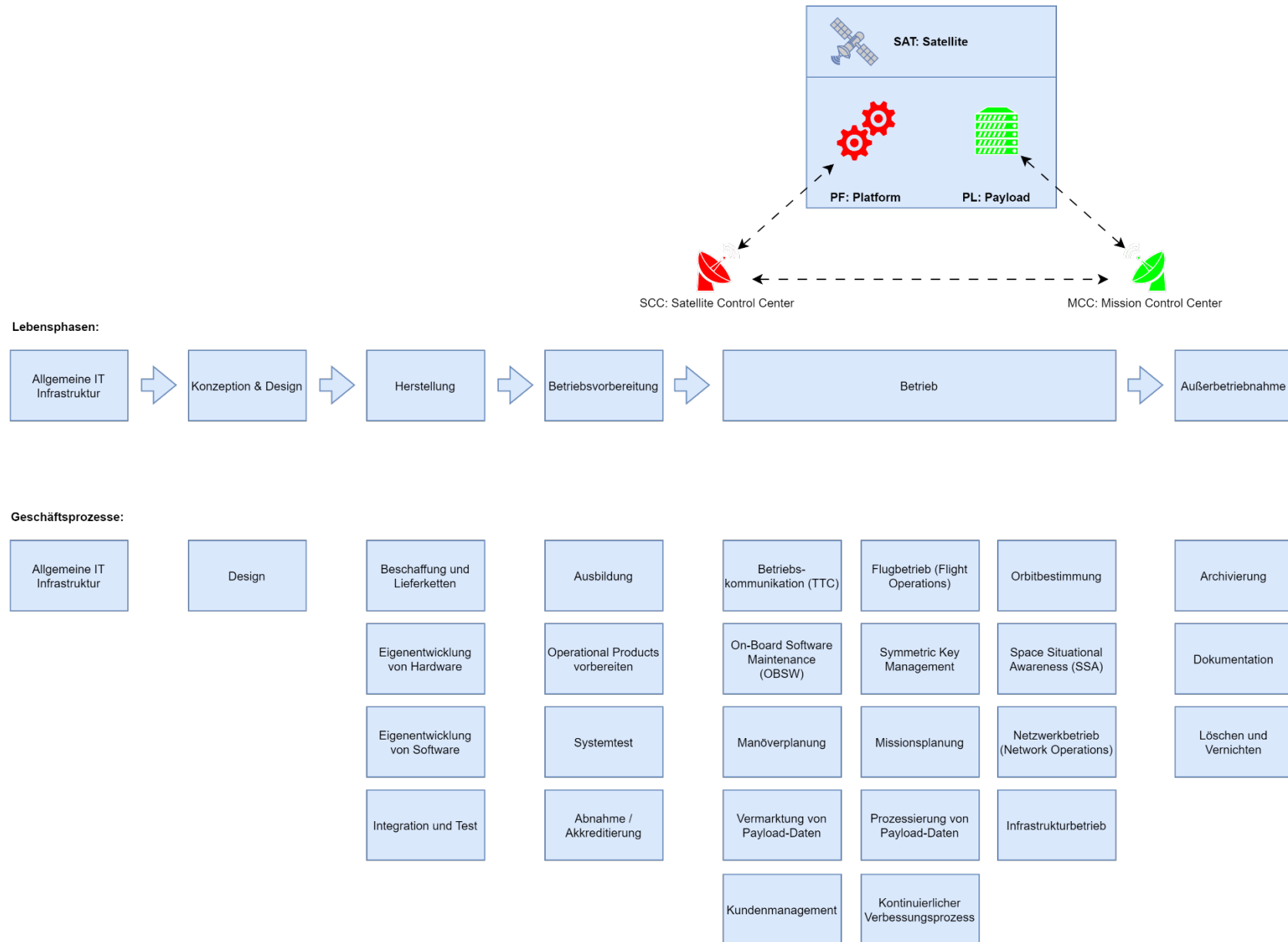


Abbildung 2: Zusammenhang von Bodensegment, Lebensphasen und Geschäftsprozessen

8.1.1 Allgemeine IT-Infrastruktur

Für den Betrieb des Unternehmens wird allgemeine, nicht-weltraumspezifische IT-Infrastruktur benötigt. Der GP „Allgemeine IT-Infrastruktur“ dient der Erfassung dieser übergreifenden Systeme und Anwendungen. Darunter fallen Aufgaben wie Kommunikation, Dokumentation, Datenablage, Datensicherung, Schutz vor Schadsoftware. Dieser in der Strukturanalyse aufgeführte GP wird nicht als gesonderte Lebensphase betrachtet, er dient der Erfassung von Standard-IT und -Anwendungen.

8.1.2 Lebensphase 1: Konzeption und Design

In dieser Phase werden Studien durchgeführt und die Projektstruktur aufgebaut, d.h. es werden Konsortien gebildet, Subunternehmer, Zulieferer und Entwickler ausgewählt. Die Feinabstimmung der Projektrealisierung und Meilensteine werden festgelegt.

GP101 Design

Alle vorbereitenden Aktivitäten für die Herstellungsphase, sodass das Bodensegment vollständig definiert ist, müssen am Ende des Prozesses abgeschlossen sein.

8.1.3 Lebensphase 2: Herstellung

In dieser Phase wird das geplante Bodensegment realisiert. Innerhalb dieser Lebensphase werden unterschiedliche Teilprozesse betrachtet.

GP201 Beschaffung und Lieferketten

Dieser Prozess gewährleistet die kontinuierliche Verfügbarkeit sämtlicher erforderlicher Komponenten des Bodensegments über den gesamten Zeitraum der Mission, indem diese bereitgestellt und instandgehalten werden.

Dabei kann die Hersteller- und Lieferantenauswahl durch gesetzliche Vorgaben (z.B. Export-/Import-Richtlinien) eingeschränkt sein. Bei KRITIS relevanten Missionen sind u.U. zusätzlich gesetzliche Lieferkettenanforderungen zu erfüllen. Ergänzt wird dieser Prozess mit der Sicherstellung geeigneter Transportwege/-mittel/-unternehmen und Wareneingangsprüfungen.

GP202 Eigenentwicklung von Software

Dieser GP betrifft die eigene Entwicklung bzw. Anpassung von Hardware und Software und kann dem Baustein CON.8 folgend bearbeitet werden.

GP203 Eigenentwicklung von Hardware

Dieser Prozess behandelt die Eigenentwicklung von Hardware für das Bodensegment. Der Prozess ist zu berücksichtigen, wenn Hardwarekomponenten angefertigt oder Zulieferer mit der Anfertigung von Hardware beauftragt (z.B. Konsolen, Antennen, etc.) werden.

GP204 Integration und Test

In diesem Prozess werden einzelne Komponenten zu einem (Teil-) System bis hin zum fertigen Bodensegment integriert. Die Tests umfassen sowohl Komponenten- als auch Systemtests. Das Bodensegment wird hierbei iterativ integriert und getestet.

8.1.4 Lebensphase 3: Betriebsvorbereitung

In beide Richtungen existieren Schnittstellen und Überschneidungen der Prozesse. Während des Herstellungsprozesses können bereits Betriebsvorbereitungen erfolgen. Gleichzeitig können zeitliche Überschneidungen zwischen den Betriebsvorbereitungen und dem Betrieb auftreten.

GP301 Ausbildung

Das Betriebspersonal wird auf Routineaufgaben sowie in der Behandlung von Notfallszenarien ausgebildet. Hier ist eine Abstimmung zwischen Herstellung und Betrieb, unter anderem für die Rolleneinteilung und Notfallbehandlung notwendig.

GP302 Operationelle Produkte vorbereiten

Erstellung und Validierung aller für den Flugbetrieb benötigten Produkte (z.B. Verfahrensanweisungen/Prozeduren) inklusive der unterstützenden Werkzeuge.

GP303 Systemtest

Möglichst umfassende Ende-zu-Ende Tests des Weltraumsystems (z.B. System Validation Test (SVT)) stellen sicher, dass das Bodensegment mit dem Raumsegment technisch kompatibel ist und die geplanten Prozeduren wie vorgesehen funktionieren. Details können abgestimmt und mögliche erkannte Fehler behoben werden.

GP304 Annahme/Akkreditierung

Je nach Anspruch bzw. Anforderungen an das Bodensegment können formelle Abnahmen, Zertifizierungen, Akkreditierungen, etc. notwendig sein (z.B. Überprüfung baulicher Eigenschaften, VS-Konformität und Penetration Tests).

8.1.5 Lebensphase 4: Betrieb

In dieser Phase wird das Raumsegment über das Bodensegment betrieben und somit die Lebensphasen Inbetriebnahme, Betrieb und Außerbetriebnahme des Raumsegments begleitet. Alle Maßnahmen der Betriebsvorbereitung sind abgeschlossen. Ggf. werden Leistungen aus Service und Wartungsverträgen erbracht, sodass während des Betriebs Schnittstellenprozesse aus den vorhergegangenen Lebensphasen mitwirken (z.B. Tests beim Einbringen von Änderungen und Patches).

GP401 Orbitbestimmung (Orbit Determination)

Dieser Prozess dient zur regelmäßigen Berechnung der aktuellen Orbitparameter aller Satelliten der Mission. Die notwendigen Daten können aus verschiedenen Quellen kommen, z.B. aus Trackingdaten von TTC-Bodenstationen oder aus Telemetriedaten der Satelliten (falls GNSS-Empfänger an Bord verwendet werden). Die aktuellen Orbitparameter werden anschließend auch zur Orbitvorhersage (Orbit Prediction) verwendet.

GP402 Missionsplanung

Dieser Prozess erzeugt regelmäßig den „Arbeitsplan“ für das Weltraumsystem. Wiederkehrende Aufgaben (z.B. Wartungstätigkeiten und Orbitkorrekturen) und spezielle Aufgaben (z.B. On Board Software (OBSW) Updates) müssen im Missionszeitplan vorgesehen werden, Anfragen aus dem Nutzerbodensegment (z.B. Erdbeobachtungsanfragen von Kunden) werden auf Plausibilität geprüft und in den Zeitplan integriert. Je nach Komplexität des Systems können auch in diesem Prozess Simulationen notwendig sein, um das geplante Zusammenspiel aller Aktivitäten vorab zu validieren.

GP403 Flugbetrieb (Flight Operations)

Dieser Prozess umfasst die operative Schnittstelle des Bodensegments zum Raumsegment. Die TM („Downlink“) Daten der Satelliten werden hier verarbeitet und ausgewertet („Health Checks“). In anderer Richtung („Uplink“) wird der Satellit durch Telekommandos kommandiert. Das Betriebspersonal nutzt hierfür das Mission Control System (MCS) als zentrale Komponente. Alle Aktivitäten sind prozedural durch die operationellen Produkte geprägt.

Einige Unterprozesse des Flugbetriebs werden in dedizierten GP betrachtet, um deren besonderer Bedeutung Rechnung zu tragen.

GP404 On-Board Software Maintenance

Auch nach dem Start eines Satelliten sollte die On-board Software (OBSW) weiterhin gepflegt und aktualisiert werden können. Dieser Prozess kann für die IT-Sicherheit technisch sehr komplex sein, da die verschiedenen Einzelaufgaben häufig durch unterschiedliche Parteien übernommen werden. Die neue OBSW wird entwickelt und getestet, sie wird vom Entwickler zum Betreiber geliefert, dort werden die Patches nochmals geprüft (i.d.R. auch mit Satelliten-Simulatoren). Nach der zeitlichen Einplanung werden die Patches auf den Satelliten geladen und aktiviert. Hier kann es prozessuale Schnittmengen mit dem Flugbetrieb und der Missionsplanung geben.

GP405 Key Management

Beschreibt Systeme und Anwendungen, welche beim Austausch der Schlüssel für die Kommunikation SAT-Boden/Boden-SAT benötigt werden.

GP406 Telemetry, Tracking and Command (TTC)

Dieser Prozess umfasst die Ende-zu-Ende-Telekommunikationsverbindung zwischen MCS und Raumsegment. Sind TTC-Bodenstationen im Einsatz, gehören die Sammlung und Übermittlung von Trackingdaten ebenfalls in diesen Prozess.

GP407 Space Situational Awareness (SSA)

Dieser GP soll sicherstellen, dass ein Betreiber den Zustand der Umgebung in seinem Raumsegment kennt und so die Möglichkeit hat, bei Gefährdungen reagieren zu können. Zu möglichen Gefährdungen zählen u.a. Weltraumwetter, weitere Objekte in ähnlichen Umlaufbahnen und Near-Earth Objects (NEO). Drei wesentliche Aktivitäten sind hierfür zu erwähnen:

- Sammeln von Informationen (z.B. Orbitdaten anderer Raumsegmente sowie Weltraumwetter),
- Bereitstellen eigener Informationen an andere Betreiber bzw. an SSA-Koordinierungsstellen (z.B. eigene Orbitdaten),
- Bereitschaft zur Kommunikation mit anderen Betreibern im Falle einer möglichen Kollision, um Ausweichaktivitäten zu koordinieren.

GP408 Kontinuierlicher Verbesserungsprozess

Während der Betriebsphase werden Mitarbeitende ständig weitergebildet und sensibilisiert. Die Flugprozeduren werden weiter verbessert und das Betriebspersonal wird durch regelmäßiges Training (auch im Simulator) geschult, weitergebildet und auf verschiedene Szenarien vorbereitet. Auf technischer Ebene werden identifizierte Anomalien untersucht und organisatorische oder technische Lösungen in die Betriebsprozesse eingebracht.⁴

GP409 Netzwerkbetrieb (Network Operations)

Dieser GP umfasst Netzwerkverbindungen und Netzwerkmanagement der verteilten Systeme (z.B. zwischen Bodenstationen und Kontrollzentrum, aber auch zwischen Kontrollzentrum und Herstellern, SVT).

GP410 Manöverplanung

Dieser Prozess umfasst sowohl planbare Manöver (Orbit-Korrekturen: Station Keeping / Orbit Correction), als auch spezielle Manöver (z.B. Kollisionsvermeidung: Collision Avoidance). Die Manöver werden anschließend im GP402 Missionsplanung im Missionszeitplan berücksichtigt, bei kurzfristigen Ausweichmanövern kann die Abkürzung direkt zum GP403 Flugbetrieb notwendig sein.

GP411 Infrastrukturbetrieb

Neben Wartungstätigkeiten und Reparaturen im Bodensegment umfasst dieser GP Software-Updates und Patch-Management. Ausgeführte Tätigkeiten und Konfigurationsänderungen werden dokumentiert. Entdeckte Mängel in geplanten Lieferketten für Ersatzteile werden hier ebenfalls behandelt.

GP412 Verarbeitung von Payload-Daten

Stellt das Bodensegment auch den Service für Download und Verarbeitung von Payload-Daten bereit, fallen die notwendigen Aktivitäten unter diesen GP.

GP413 Kundenmanagement

Wirtschaftliche Aktivitäten, die bei kommerziellen Weltraumsystemen mit der Betreuung von Kunden zu tun haben (z.B. Akquise, Customer-Relationship-Management (CRM), Kundenportale, Kundensupport) werden in diesem GP abgedeckt.

⁴ Vgl. Kapitel 10.5 Business Continuity Management (BCM)

GP414 Vermarktung von Payload-Daten

Dies umfasst bei kommerziellen Weltraumsystemen alle Aktivitäten, die mit der Bestellung und Auslieferung von (verarbeiteten) Payload-Daten an Nutzer/Kunden zu tun haben.⁵

8.1.6 Lebensphase 5: Außerbetriebnahme

Nach der Außerbetriebnahme des Raumsegments (Passivation und ggf. Deorbit-Manöver) kann das Bodensegment außer Betrieb genommen werden. Die hier aufgeführten GPs existieren ebenfalls bei sog. Teil-Außerbetriebnahmen. Enthalten ist in diesem GP der Umgang mit ausgemusterten Komponenten und Daten nach einem Upgrade des Bodensegments, z.B. nach Upgrade des Raumsegments durch Satelliten einer neueren Generation.

GP501 Löschen und Vernichten

Komponenten und Daten, welche nach Missionsende nicht weiter benötigt werden, sollten gelöscht oder vernichtet werden. Hier sind u.U. gesetzliche Aufbewahrungsfristen und Datenschutzregelungen zu beachten.

GP502 Archivierung

Daten, welche nach Missionsende nicht gelöscht werden, müssen entsprechend ihrer Einstufung archiviert werden. Hier sind u.U. gesetzliche Aufbewahrungsfristen und Datenschutzregelungen zu beachten.

GP503 Dokumentation

Die Außerbetriebnahme ist vor der Durchführung zu planen und zu dokumentieren. Zusätzlich ist die Durchführung der Außerbetriebnahme ggf. zu dokumentieren, um eine Nachvollziehbarkeit über die Löschung oder Speicherung von Informationen sicherzustellen.

8.2 Anwendungen

Zu dem Informationsverbund gehören neben den Prozessen außerdem die Anwendungen, die eine Bearbeitung dieser Prozesse unterstützen.

Allgemeine IT-Infrastruktur umfasst GP-übergreifende Systeme und Anwendungen. Darunter fallen Systeme für Kommunikation, Dokumentation, Datenablage, Datensicherung, oder Schutz vor Schadsoftware. Spezielle Anwendungen erlauben den Betrieb des Satelliten und unterstützen beispielsweise die Missionsplanung und -kontrolle, Simulation oder Schulung des Bedienpersonals.

Eine vollständige Liste der Anwendungen für das Bodensegment, sowie die jeweils zugehörigen Lebensphasen und GP sind im Annex Strukturanalyse zu finden.

8.3 IT-Systeme

Die in einem Informationsverbund benötigten Anwendungen werden auf IT-Systemen ausgeführt. Darüber hinaus beinhaltet ein Informationsverbund auch andere IT-Systeme, die nicht unmittelbar für die Ausführung der eigentlichen Anwendungen benötigt werden. Beispiel dafür sind Netzkomponenten wie Switches.

Eine vollständige Liste der IT-Systeme für das Bodensegment ist im Annex Strukturanalyse zu finden.

8.4 Netze und Netzkomponenten

Anwendungen und IT-Systeme des Informationsverbundes „Bodensegment“ sind in verschiedene Netzwerke eingebunden. Auch wenn sich Anzahl und Aufbau der Netze nicht im Detail verallgemeinern

⁵ Für GP412, 413 und 414 gilt: Die Payload wird in diesem Dokument nicht direkt betrachtet. Es kann missionsbedingt notwendig sein, durch Art und Weise der Verarbeitung von Payload- und Plattforminformationen, die möglichen Schnittmengen von IT-Systemen und Anwendungen auch zu betrachten.

lassen, wird davon ausgegangen, dass die Architektur vieler Missionen hinsichtlich Netze und Netzkomponenten zumindest ähnlich ist.

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

8.5 Gebäude und Räume

Wie gut Informationen und Informationstechnik geschützt sind, hängt immer auch von der Sicherheit der räumlichen Umgebung ab, in denen das Bodensegment oder damit verbundene Systeme oder Komponenten hergestellt, getestet und betrieben werden oder Mitarbeitende tätig sind. Daher sind auch alle Gebäude und Räume bei einer Absicherung nach IT-Grundschutz zu berücksichtigen.

Eine Liste der möglichen Gebäude und Räume ist im Annex Strukturanalyse zu finden.

9 Modellierung

Im Annex Strukturanalyse sind alle für den exemplarischen Informationsverbund relevanten IT-Grundschutz-Bausteine aufgeführt und den jeweiligen Zielobjekten zugeordnet. Die Zuordnung ist exemplarisch. Die Anwender des IT-Grundschutz-Profils müssen überprüfen, ob ihr jeweiliger Informationsverbund vom dargestellten Muster-Informationsverbund abweicht.

Abhängig von den tatsächlichen Gegebenheiten können für bestimmte Zielobjekte andere IT-Grundschutz-Bausteine relevant sein. Beispielsweise können Anwendungen als Desktopanwendung oder Webanwendung konzipiert sein. In diesem Fall sind jeweils andere Bausteine des IT-Grundschutz-Kompendiums auszuwählen.

In der Praxis kommt es außerdem oft vor, dass nicht jedem Zielobjekt zutreffende IT-Grundschutz-Bausteine zugeordnet werden können. In diesem Fall muss eine Risikoanalyse (siehe Kapitel 10.4 Risikomanagement) durchgeführt werden, bei der für das Zielobjekt geeignete Bewältigungsmaßnahmen ausgewählt werden.

Neben den IT-Grundschutz-Bausteinen, die konkreten Zielobjekten zugeordnet wurden, gibt es außerdem weitere IT-Grundschutz-Bausteine, die übergreifend angewendet werden müssen. Diese befassen sich beispielsweise mit organisatorischen Aspekten und müssen auf den Informationsverbund als solchen angewendet werden.

Eine vollständige Liste der identifizierten Bausteine ist im Annex Strukturanalyse zu finden.

10 Spezifische Hinweise

Dieses IT-Grundschutz-Profil bietet eine Hilfestellung für die Implementierung und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) für Bodensegmente. Da die Sicht des BSI IT-Grundschutzes und anderer gängiger Normen i.d.R. von Bestandssystemen, etablierten Prozessen und Systemen ausgeht, gibt es durchaus Besonderheiten und Prozesse, die in den Lebensphasen Konzeption und Design sowie Herstellung des Systems zusätzlich erwähnt werden sollten. Die Erfahrungen der Industrie dienen als Hilfestellung, um Prozesse zu optimieren. Die Industrie geht an dieser Stelle davon aus, dass Raum- als auch Bodensegmente über Projekte realisiert werden. In diesen Projekten wird die Entwicklung eines Bodensegmentes als Produkt betrachtet, das potenziellen Kunden zum Kauf angeboten wird.

10.1 Prozesslandschaft und Verantwortungen

Neben technischen Erwägungen hat die Art der Organisation ebenfalls großen Einfluss auf die Informationssicherheit. Dienstleister die (Teil-)Aufträge für den Bau und ggf. auch den Betrieb des Bodensegmentes übernehmen, bilden Prozessschnittstellen, die effektiv und effizient funktionieren müssen. Nur eine reibungslose Zusammenarbeit zwischen AG, AN und Betreiber kann eine Informationssicherheit gewährleisten.

Spezifikationsdokumente, die den Fokus auf eine klare Zuständigkeitsverteilung legen, unterstützen die Ausgestaltung der Arbeitsabläufe zwischen AG und AN. Diese Spezifikationsdokumente müssen in lückenlose Prozesse und Prozeduren überführt und verpflichtend anwendbar gemacht werden.

Bei der Planung und Umsetzung des ISMS ist eine regelmäßige und enge Abstimmung zwischen allen beteiligten Stakeholdern erforderlich. Ein effektives Qualitätsmanagement muss die Validierung, Weiterentwicklung aber auch die Einhaltung aller Prozesse und Prozeduren über den gesamten Lebenszyklus sicherstellen.

10.2 Externe Dienstleistungen

Im Missionsdesign sind eine Vielzahl von make-or-buy Entscheidungen zu treffen. Dies betrifft nicht nur Komponenten, sondern auch komplette Teil-Leistungen der Bodeninfrastruktur. Beispielfhaft seien Antennennetzwerke „as a Service“, SaaS oder Cloud-Dienstleistungen erwähnt. Hierbei ist, analog zur Lieferkettensicherheit, der Anbieter gemäß der eigenen Sicherheitsansprüche auszuwählen, in die Definition und Entwicklung aller nötigen Schnittstellen einzubinden und regelmäßig zu auditieren. Eine Herausforderung kann dabei sein, dass Schnittstellen und Servicezusagen durch die jeweiligen Anbieter bereits starr vorgegeben werden. Resultierend muss eine detaillierte Risikoabschätzung in die make-or-buy Entscheidung sowie in die Auswahl geeigneter Dienstleister einfließen.

Dienstleistungen von Dritten müssen geprüft werden. Bei der Risikoanalyse (siehe 10.4 Risikomanagement) ist die Kritikalität der Schnittstelle im Hinblick auf die Exposition des Systems nach außen zu berücksichtigen. In gleicher Weise ist jeder Dienstleister im Hinblick auf das Vertrauen und den Cyber-Reifegrad des Unternehmens zu bewerten. Es muss auch sichergestellt werden, dass die Dienstleistungsvereinbarung zwischen den Parteien auch die Sicherheitsaspekte berücksichtigt. Eine detaillierte Beschreibung der Schnittstelle, der Protokolle und des Datenaustauschs ist in einem Dokument zur Kontrolle externer Schnittstellen zu dokumentieren.

Es hat sich bewährt, Vorlagen für den Austausch sensibler Daten wie IP-Adressen, Portnummern oder sogar Schlüsselmaterial zu vereinbaren. Bei der Übermittlung sensibler Daten sind die Grundsätze „Kenntnis nur, wenn nötig“ und „geringste Funktionalität“ zu beachten. In der Regel handelt es sich um einen Austausch zwischen Sicherheitsbeauftragten und der Dateiaustausch erfolgt verschlüsselt.

10.3 Betriebskommunikation

Eine essenzielle Aufgabe des Prozesses „Betriebskommunikation (TTC)“ ist es, zuverlässige Telekommunikationsverbindungen zwischen dem MCS und dem Raumsegment herzustellen.

Zur Sicherstellung der Vertraulichkeit ist hierfür eine Ende-zu-Ende Verschlüsselung der Kommunikation zwischen MCS und Plattform zu empfehlen. Je nach Missionstyp und AG kann dies auch (z.B. mit entsprechend zertifizierten Kryptolösungen) gefordert sein. Ein positiver Effekt dieser Ende-zu-Ende Verschlüsselung ist, dass alle Komponenten zwischen MCS und Plattform (z.B. die Bodenstationen, aber auch unerwünschte Mithörer) nur verschlüsselte Daten zu sehen bekommen. Somit schwächt die Nutzung von Bodenstationen, welche nicht unter eigener Kontrolle stehen (Groundstation-as-a-Service), die Vertraulichkeit der Kommunikation in keiner Weise.

Eine weitere Herausforderung, ist die Sicherstellung der Verfügbarkeit der Kommunikationsverbindungen im Element der TTC-Bodenstationen.

Die für eine Mission geeigneten TTC-Bodenstationen befinden sich möglicherweise an unzugänglichen Orten (z.B. liegen die für Missionen in LEO an den geeignetsten TTC-Bodenstationen in polaren Regionen). Einerseits kann dies einen Perimeterschutz (gegen physische Sabotage) aufgrund der beschränkten Zugangsmöglichkeiten erleichtern, andererseits werden - aus denselben Gründen - Installation, Instandhaltung und Reparaturarbeiten und den Bodenstationen erschwert. Dieser Aspekt sollte bei der Planung des Standortes und den anvisierten Einsatzzeiten berücksichtigt werden, um die benötigte Verfügbarkeit der Betriebskommunikation sicherzustellen.

Härtung und Redundanzen innerhalb der Bodenstationen erhöhen hier die Ausfallsicherheit, aber auch zusätzliche Bodenstationen (z.B. Anmieten bei Groundstation-as-a-Service Anbietern) verbessern die Verfügbarkeit. Unbemannte Bodenstationen können während planbaren kritischen Operationen (z.B. Launch and Early Orbit Phase (LEOP)) auch temporär bemannt werden.

10.4 Risikomanagement

Ein Risikomanagementsystem (RMS) stellt sicher, dass eine Institution gesetzliche und regulatorische Anforderungen im Bereich der Informationssicherheit erfüllt und somit das Risiko von Sanktionen und Reputationsschäden minimiert werden kann.

Dem zur Folge ist die Implementierung eines effektiven RMS von entscheidender Bedeutung für Institutionen, die sich den Herausforderungen der Informationssicherheit stellen müssen. Ein wirksames RMS identifiziert, analysiert und bewertet potenzielle Risiken für die Informationssicherheit. Hierfür bietet der *BSI-Standard 200-3: Risikomanagement*⁶ eine Methodik. Nachfolgend sind zusammenfassend die Schritte einer Risikoanalyse, als Bestandteil eines RMS, kurz aufgeführt:

- Erfassung der Zielobjekte,
- Erstellung einer Gefährdungsübersicht,
- Ergänzung der Gefährdungsübersicht,
- Bewertung der Häufigkeit und Schadensauswirkungen,
- Bewertung der Risiken,
- Behandlung der Risiken,
- Konsolidierung der Sicherheitskonzeption.

⁶ Die Methodik ist im BSI-Standard 200-3 als Onlinedokument unter <https://www.bsi.bund.de/dok/10027822> (Stand: 09.02.2024) verfügbar.

Als Hilfsmittel für die Identifizierung von Gefährdungen für eine durchzuführende Risikoanalyse stehen u.a. Übersichten bzw. Frameworks zur Verfügung:

- BSI - Elementare Gefährdungen
(URL: <https://www.bsi.bund.de/dok/10099762/>, Stand: 09.02.2024),
- ESA - Space Attacks and Countermeasures Engineering Shield (SPACE-Shield)
(URL: <https://spaceshield.esa.int/>, Stand: 09.02.2024),
- The Aerospace Corporation - Space Attack Research and Tactic Analysis (SPARTA)
(URL: <https://sparta.aerospace.org/>, Stand: 09.02.2024),
- Mitre Corporation - Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
(URL: <https://attack.mitre.org/>, Stand: 09.02.2024).

Die Implementierung eines RMS ist nicht statisch, sondern ein iterativer Prozess. Regelmäßige Kontrollhandlungen, Bewertungen und Anpassungen sollen ein effektives RMS gewährleisten, welches als proaktiver Anteil in einer Sicherheitsarchitektur gesehen werden kann.

In diesem Zusammenhang ist es u.a. empfehlenswert eine gemeinsame Risikobetrachtung zwischen dem AG und AN festzulegen, um Risiken einheitlich zu evaluieren bzw. zu behandeln. Hierzu zählt die Entscheidung auf *eine* gültige Risikomethodik und somit die Auswahl auf *einen* entsprechenden RM-Standard. Die iterative Risikobetrachtung innerhalb des Projektfortschritts ist obligatorisch; insbesondere die Betrachtungen die sich auf die *Nichtumsetzung*⁷ von Informationssicherheitsvorgaben beziehen. In Systemspezifikationen werden bspw. die auf das System anzuwendenden Informationssicherheitsvorgaben festgehalten.

Die umfassende Erfüllung sämtlicher zwischen AG und AN vereinbarter Informationssicherheitsvorgaben, gemäß den Systemspezifikationen, kann eine anspruchsvolle Aufgabe darstellen – insbesondere die Nichtumsetzung von Vorgaben im Rahmen der Systemrealisierung. Dies kann z.B. aus Gründen der Systemperformance oder aus Gründen der Systemstabilität bedingt sein. Die Risiken sind unter Anwendung der entsprechend abgestimmten Methoden zu identifizieren und mit geeigneten Schutzmaßnahmen zu versehen. Restrisiken sind zu evaluieren und die Dokumentation ist in einem Risikoregister zu erfassen. Falls erforderlich, ist eine regelmäßige Revalidierung des Risikos im Risikoregister vorzunehmen. Für diese Tätigkeiten ist der Risikoeigentümer⁸ verantwortlich.

10.5 Business Continuity Management

In diesem Kapitel wird nicht jede Lebensphase bzw. nicht jeder GP vollumfänglich aus Sicht der Notfallvorsorge bzw. aus Sicht möglicher reaktiver Maßnahmen behandelt. Es werden jedoch einige Best Practice Ansätze aufgeführt, die im Rahmen des Notfallmanagement umgesetzt werden sollten.

Bodensegmente sind für die Satellitensteuerung bzw. Kommandierung unerlässlich. Ein kontinuierlicher Betriebsablauf, beginnend mit der Startphase bis hin zum gezielten De-Orbiting durch Kommandos und Manöver, die vom Bodensegment initiiert werden, ist von entscheidender Bedeutung. Unterbrechungen in der Kommunikation zwischen Raum- und Bodensegment über längere Zeiträume hinweg bergen erhebliche Risiken. Selbst ein Verlust eines Satelliten kann ohne gezielte Maßnahmen zur Aufrechterhaltung der betrieblichen Kontinuität nicht ausgeschlossen werden. Die Betriebsstabilität verbessert sich erheblich durch den Einsatz eines auf die Projektorganisation bzw. auf das Produkt abgestimmten Notfallmanagements.

⁷ Als Beispiel wäre die Entscheidung zur Nutzung von http statt https in einem unkritischen Systembereich aufgrund der zu erwartenden Performanceeinschränkungen zu nennen.

⁸ Im Risikomanagement werden Rollen und Verantwortlichkeiten benannt und direkt zugewiesen.

Insgesamt trägt ein Business Continuity Management (BCM) dazu bei, die Kontinuität der Operationen des Informationsverbundes im Bodensegment sicherzustellen, und gewährleistet die Zuverlässigkeit und Stabilität von Missionen.

Ein BCM stellt mit Maßnahmen aus Notfallvorsorge und reaktiver Maßnahmen sicher, dass die Kommunikation selbst unter extremen Bedingungen (z.B. kurzer oder längerfristiger Ausfall der lokalen Energieversorgung, Störungen oder technische Defekte und ggf. weiteren Eskalationsstufen) aufrechterhalten wird, um Datenübertragungen, Kontrolloperationen und Flugmanöver zu gewährleisten.

Bodensegmente können an verschiedenen Orten auf der Erde stehen, und sie müssen u.a. gegen Naturkatastrophen wie Erdbeben, Stürme oder Überschwemmungen geschützt sein.⁹ Die physische Erreichbarkeit, beeinflusst durch lokale Gegebenheiten, kann ebenfalls eine erhebliche Herausforderung für die kontinuierliche Betriebsführung von Bodensegmenten darstellen. In diesem Kontext wird dem BCM eine entscheidende Rolle zuteil, indem es Maßnahmen aus der Notfallvorsorge konzipiert und implementiert, um einen ununterbrochenen Betrieb trotz solcher und weiteren Herausforderungen zu gewährleisten.

Der BSI-Standard 200-4¹⁰ bietet eine praxisnahe Anleitung für das BCM, um auf Krisensituationen angemessen reagieren zu können.

Die wesentlichen Elemente eines BCM können wie folgt zusammengefasst werden:

- Identifikation kritischer GP und Ressourcen,
- Entwicklung von Notfallplänen und Wiederherstellungsstrategien,
- Regelmäßige Notfallübungen, Schulungen und Tests, um die Wirksamkeit der Maßnahmen zu überprüfen; die Schulung der Mitarbeiter soll eine schnelle und koordinierte Reaktion auf Notfälle gewährleisten.

Das Notfallmanagement konzentriert sich auf die unmittelbare Reaktion in kritischen Situationen, um das Schadensausmaß zu begrenzen bzw. den Betrieb und die wichtigsten Prozesse aufrechtzuerhalten und, falls erforderlich, den Betrieb wiederherzustellen.

Eine grundlegende Anforderung an das Betriebsbodensegment, welches im Notfallmanagement zu berücksichtigen ist, leitet sich direkt aus einer typischen Anforderung an das Raumsegment ab: Wie lange soll das Raumsegment ohne Verbindung zum Betriebsbodensegment (also autonom) „überleben“ können?

Eine ausbleibende Betriebskommunikation wird i.d.R. dazu führen, dass das Raumsegment den Nutzlastbetrieb einschränken bzw. einstellen muss; bei noch längerem Ausbleiben der Betriebskommunikation wird das Raumsegment gezwungen sein, autonom auch Rekonfigurationen an seiner Plattform durchzuführen, um tatsächlich seine Überlebenschancen zu erhöhen.

Daraus ergibt sich also ein Recovery Time Objective (RTO) an das Notfallmanagement.

In Projekten und für den operativen Systembetrieb eines Bodensegments (relevant für Missionen) konzentrieren sich die Tätigkeiten i.d.R. auf die Themen der Notfallvorsorgemaßnahmen und auf reaktive Maßnahme. Letztere werden in einem für den Betrieb erforderlichen Notfallhandbuch¹¹ aufgeführt.

⁹ Die Gefährdungen werden im Risikomanagement ermittelt und in der Risikoanalyse als Risiken identifiziert, bewertet und mit angemessenen Schutzmaßnahmen versehen. Siehe Kapitel 10.4

¹⁰ Die Vorgehensweise ist im BSI-Standard 200-4 als Onlinedokument unter <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4-Business-Continuity-Management-node.html> (Stand: 09.02.2024) verfügbar.

¹¹ Hierunter werden konkrete Handlungsanweisungen verstanden die einen direkten Bezug zur Aufrechterhaltung der Systemstabilität und -kontinuität aufweisen.

So sind Bodensegmente zum Zweck der eigenen Resilienz bspw. mit mehreren Redundanzen zu versehen, um in einem Notfall eingreifen oder um auf einen potenziellen Notfall frühzeitig reagieren zu können. Hierzu zählt insbesondere ein zusätzlicher Notfallarbeitsplatz, von dem aus der Satellit kommandiert und in seiner Umlaufbahn gehalten werden kann. Diese funktionale Sicherheitsanforderung - ggf. auf die Steuerung beschränkt, bestimmt das genaue Vorgehen in einem erforderlichen Manöver. Fällt zeitgleich der Hauptstandort für die Kommandierung aus, erfordert dies zusätzliche Manöver und somit bedingt den Wechsel auf den Notfallarbeitsplatz, der geografisch und räumlich getrennt vom Hauptstandort verfügbar sein muss. Funktionale Sicherheitsanforderungen lassen sich durch technische systemseitige Sicherheitsvorgaben sinnvoll ergänzen. Insbesondere in der LEOP - im Rahmen von Satellitenstarts - kann dieser Arbeitsplatz im Bodensegment ein wichtiges Steuerungselement bis zur vollständigen Übergabe an den Satellitenbetrieb darstellen. Die zur Steuerung relevanten Systemkomponenten müssen dabei redundant ausgelegt werden.

Für eine nachhaltige Implementierung des Notfallmanagementprozesses sollte eine Business Impact Analyse (BIA) im frühen Projektverlauf durchgeführt werden. Dies dient der Identifizierung der wichtigsten Kernprozesse innerhalb des Projektfortschrittes, um eine *Entscheidungsgrundlage für die Bestimmung der Dauer von Ausfallzeiten der wichtigsten Kernprozesse im Projekt* zu schaffen. Nachfolgend werden die *zeitlichen Abstände der Wiederanlaufzeiten festgelegt*, anhand derer angemessene Notfallmaßnahmen implementiert werden müssen. Im Rahmen einer durchgeführten BIA lässt sich u.a. feststellen, dass bspw. die In-Orbit-Phase einen signifikanten Anteil des kritischen Pfads im Projekt darstellt. Eine Evaluierung wirksamer Maßnahmen kann je nach Einschätzung der BIA und Risikoanalyse in Relation zur Schutzbedarfsfeststellung entstehen. Je nach Einschätzung können u.a. folgende Best Practice Ansätze zur Anwendung kommen:

- Redundante Auslegung kritischer Systemkomponenten des Notfallarbeitsplatzes und des Hauptsystems,
- Redundante Kommunikationsverbindungen z.B. Datenstandleitung des Gebäudes oder der Wechsel auf ein alternatives Frequenzband für die Aufrechterhaltung der Satellitenkommunikation,
- Notfallstromgenerator und Einsatz von unterbrechungsfreier Stromversorgung (USV) zur Sicherstellung des Energiemanagements,
- Benennung und Etablierung der Rolle „Notfallmanager“ bzw. eines „Notfallkoordinators“ sowie die Einrichtung einer ganzheitlichen Notfallmanagementorganisation inkl. Krisenstab,
- Durchführung regelmäßiger Notfalltests (z.B. Systemwechsel von Standort A zu Standort B inklusive Betriebsaufnahme, Kommandierung und Steuerung), Notfallschulungen sowie Lessons Learned Workshops und
- Sicherstellung von ausreichenden personellen Ressourcen.

11 Missionsmerkmale

Der Schutzbedarf einer Mission in ihrer Gesamtheit wirkt auf alle für die Mission notwendigen Anwendungen, Systeme, Netze, Räume und Gebäude. Der Schutzbedarf kann sich in den einzelnen Lebensphasen und Prozessen unterscheiden und muss daher jeweils angepasst bzw. überprüft werden.

Beispielsweise ist die Verfügbarkeit eines Systems im GP204 „Integration und Test“ nicht von hoher Priorität, da das System auch so weit penetriert werden kann, dass es zum Ausfall gebracht wird. So lassen sich in einer frühen Phase Schwachstellen und Probleme erkennen. Im Vergleich dazu ist z.B. in der Lebensphase „Betrieb“ i.d.R. die Verfügbarkeit ein für den Geschäftszweck erforderliches Merkmal mit hoher Priorität.

Als wesentliche Merkmale für die Bewertung einer Mission wurden:

- Missionstyp,
- Orbit bzw. Erd-Umlaufbahn,
- Konstellationsgröße,
- Stakeholder/Zweck und
- Infrastruktur

identifiziert.

Der Missionstyp dient zur grundsätzlichen Beschreibung der Aufgabenstellung und definiert die Anforderungen an das Gesamtsystem. Beispiele sind Erdbeobachtung, Navigation oder Kommunikation. Der Missionstyp hat direkten Einfluss auf alle nachfolgenden Faktoren. Die betrachteten Missionsmerkmale bilden später die Grundlage für eine sachgerechte Schutzbedarfsfeststellung.

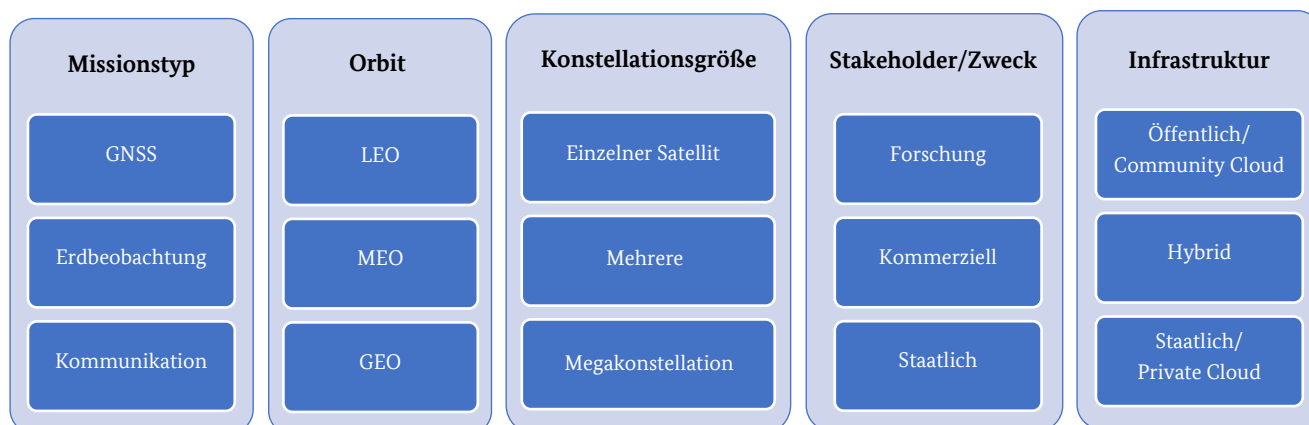


Abbildung 3: Übersicht über die verschiedenen Missionsmerkmale

Abbildung 3 zeigt, anhand welcher Missionsmerkmale eine Fallbetrachtung für das umzusetzende Projekt durchgeführt werden kann. Hierzu müssen Missionstyp, Orbit, Konstellationsgröße, Stakeholder/Zweck und Infrastruktur den Anforderungen entsprechend verbunden werden. Anhand dessen lassen sich verschiedene Anforderungen konstruieren und der Schutzbedarf an die Systeme feststellen.

11.1 Missionstyp

Im Rahmen dieses Dokuments werden Missionstypen folgender drei Gruppen betrachtet:

- Ortung, Navigation und Zeitmessung (GNSS bzw. PNT),
- Erdbeobachtung (alle Arten von Messungen, Bilder, usw.) und

- Kommunikation (Sprache sowie Daten).

Jeder Missionstyp hat charakteristische Eigenschaften in Bezug auf die Interaktion zwischen dem Raumsegment (Payload) und dem Nutzer im Bodensegment, aber auch auf die Komplexität der notwendigen Bodeninfrastruktur.

GNSS

GNSS wird hier als unidirektionaler Dienst verstanden. Das Nutzerterminal fungiert nur als Empfänger und die Payload betreibt lediglich einen Downlink zum Nutzerbodensegment. Eine Verschlüsselung dieses Signals kann eingesetzt werden, um den Dienst auf bestimmte Nutzer zu beschränken. Kryptografische Maßnahmen zum Schutz der Integrität und Authentizität der Signale können zum Schutz gegen Spoofing eingesetzt werden. Technische Maßnahmen (z.B. Frequenzspreizung) erschweren Jamming-Angriffe und erhöhen somit die Verfügbarkeit des Dienstes.

Es gibt weitere GNSS-Nutzungsfälle, die eine bi-direktionale Interaktion zwischen Kunde und Anbieter beinhalten. Diese Anwendungsfälle können im Rahmen dieser Analyse als Kommunikationsdienst betrachtet werden.

Die Bodeninfrastruktur ist häufig sehr komplex, da eine permanente Feedback-schleife zwischen dem Raumsegment und dem weltweit verteilten Bodensegment hoch genaue Zeit- und Positionsdaten ermitteln und verteilen muss.

Erdbeobachtung

Forschungs- und Erdbeobachtungsdaten werden häufig über eine dedizierte Bodenstation im Nutzerbodensegment übermittelt. Dazu gehören z.B. Bilder, Sensorsignale und Wetterdaten.

Häufig müssen Nutzer über entsprechende Schnittstellen zwischen Nutzer- und Betriebsbodensegment Dienstanfragen an den Nutzlastbetreiber stellen, die geprüft, bewertet und in den Missionszeitplan eingebettet werden. Die Sensoren der Payload werden dann die gewünschte Beobachtung zur entsprechenden Zeit durchführen und Sensordaten erzeugen.

Eine andere Art von Erdbeobachtungsmissionen (typisch für z.B. Wettersatelliten) agiert ohne bestimmte Beobachtungsanfragen durch Nutzer; hier „scannen“ die Sensoren der Payload permanent und erzeugen einen Datenstrom. Unabhängig davon, wie die Sensordaten erzeugt werden, müssen die gewonnenen Daten häufig zunächst an Bord zwischengespeichert werden, um sie bei nächster Gelegenheit über eine Bodenstation herunterzuladen und den Nutzern zur Verfügung zu stellen. Missionen mit Echtzeit-Telemetrie für Payload-Daten (typisch für Erdbeobachtung aus dem GEO) benötigen keine Zwischenspeicherung der Daten an Bord.

Auch bei diesem Missionstyp betreibt die Payload i.d.R. nur einen Downlink zum Nutzerbodensegment. Der Einsatz kryptografischer Maßnahmen zum Schutz dieser Verbindung sollte mindestens den Schutz der Integrität und Authentizität umfassen, bei kommerziellen Missionen auch die Vertraulichkeit.

Kommunikation

Telekommunikation über Satelliten findet klassisch über eine Telekommunikationsnutzlast in GEO-Satelliten statt. Diese Nutzlasten arbeiten i.d.R. als einfache Repeater, d.h. sie empfangen Signale von SATCOM-Terminals (am Boden) und senden sie verstärkt wieder zurück, wo sie von anderen SATCOM-Terminals empfangen werden können.

Dieses Prinzip wurde durch technologische Fortschritte erweitert. So sind inzwischen regenerative Nutzlasten in LEO/MEO-Satelliten weit verbreitet. Diese regenerativen Nutzlasten ermöglichen die Signalverarbeitung im Satelliten und eröffnen neue Möglichkeiten, aber auch neue Schwachstellen. Darüber hinaus ist mit dem ISL eine weitere Ebene zu berücksichtigen, da die Daten nicht nur zwischen Satelliten derselben Konstellation, sondern möglicherweise auch mit anderen Konstellationen oder Betreibern ausgetauscht werden können.

Unabhängig, wie der Telekommunikationsdienst im Raumsegment realisiert wird (GEO oder LEO/MEO, mit oder ohne ISLs), kann man im Nutzerbodensegment die Schutzziele für die Nutzerkommunikation einheitlich betrachten. Wie jeder andere Kommunikationsdienstleister stellt auch die Telekommunikation über Satelliten lediglich Verbindungen her (zwischen SATCOM-Terminals). Da der Schutz von Vertraulichkeit nur Ende-zu-Ende realisiert werden kann, kann die Umsetzung dieses Schutzziels auch weiterhin nur beim Nutzer liegen, so dass SATCOM-Netze lediglich die Integrität und Verfügbarkeit sicherstellen können und sollen.

11.2 Orbit

Dieses Profil beschränkt sich auf folgende drei Typen von Erd-Umlaufbahnen¹²:

- LEO: Low Earth Orbit (Höhe: Etwa 200 bis 2.000 km),
- MEO: Medium Earth Orbit (Höhe: 2.000 bis 35.786 km),
- GEO: Geostationary Earth Orbit (Höhe: 35.786 km).

Die Umlaufbahn beeinflusst direkt die Anzahl und die Standorte der Bodenstationen. Die Flughöhe des Satelliten beeinflusst die Sichtbarkeit und damit die Kommunikationsmöglichkeiten mit den Bodenstationen.

Die Umlaufbahn hat damit keinen Einfluss auf Vertraulichkeit und Integrität, beeinflusst aber direkt das Design zur Adressierung der Verfügbarkeitsanforderungen.

Die Umlaufbahn eines Satelliten kann als Fußabdruck auf der Erde dargestellt werden. Für jeden Beobachter an einem festen Punkt der Erde beeinflusst die Umlaufbahn eines Satelliten dessen Sichtbarkeit, d. h. die Verfügbarkeit des Satellitensignals. Bei GEO-Satelliten ist die Signalabdeckung statisch, während sie bei LEO und MEO dynamisch ist. In Bezug auf Störszenarien haben GEO-Satelliten den Nachteil, dass sie ständig über einen großen Teil der Erde sichtbar sind, was es stationären Störsendern mit großer Leistung ermöglicht, die Satellitentransponder zu „beleuchten“ und damit die Kommunikation zu stören.

LEO-Umlaufbahnen sind von Natur aus weniger störanfällig, da der Störsender Aufklärungsdaten benötigt, um zu wissen, wann und wo sich der Satellit in der Sichtlinie des Störsenders befindet. Im Falle einer Konstellation kann es sein, dass sich mehr als ein Satellit in Sichtweite befindet. Dadurch kann ein Benutzerterminal die gestörte Verbindung zum gestörten Satelliten überwinden, indem es eine neue Verbindung zu einem anderen Satelliten in Sichtweite herstellt. Andere Kommunikationstechniken wie das sog. Beam-Forming und Beam-Hopping fügen eine weitere Sicherheitsebene hinzu, da der Störsender auch die Richtwirkung der Verbindung überwinden muss, d.h. er muss nicht nur Sichtkontakt zum Satelliten haben, sondern auch innerhalb des Beleuchtungsstrahls zwischen dem Satelliten und dem Nutzerendgerät liegen.

11.3 Konstellationsgröße

Missionen mit einem oder wenigen Satelliten können temporäre oder permanente Ausfälle gar nicht oder nur sehr schwer kompensieren. Ausfälle haben oft direkten Einfluss auf das Missionsziel, da die Service-Verfügbarkeit eingeschränkt ist. Wird der Satellit dauerhaft beschädigt, kann der Service nur durch den Start eines Ersatzsatelliten wiederhergestellt werden.

Konstellationen mit mehreren hunderten oder tausenden Satelliten, sogenannte Megakonstellationen, bieten systematisch Redundanzen. Der Ausfall eines oder weniger Satelliten hat hier nur lokal begrenzte Auswirkungen und kann ggf. auch kurzfristig kompensiert werden.

¹² Die Bewegung des Raumsegments ist nicht auf diese Orbitsypen beschränkt, sondern kann z.B. auch als „Deep Space Mission“ umgesetzt werden, beispielsweise für die Exploration von Planeten.

Im direkten Zusammenhang mit dem Orbit hat daher die Größe einer Satellitenkonstellation Einfluss auf die Verfügbarkeit des Gesamtsystems bzw. der Mission.

Die Konstellationsgröße hat keinen direkten Einfluss auf Vertraulichkeit und Integrität.

Die Anzahl der Satelliten, auf die sich der Dienst stützt, spielt eine Rolle für die Verfügbarkeit des Dienstes. Die Anzahl ändert den Ansatz, wie viel Risiko bei Herstellung und Betrieb akzeptabel ist: je größer die Anzahl der Satelliten, desto geringer die Herstellungskosten pro Einheit und desto mehr werden kommerzielle Standardkomponenten (COTS) verwendet. Im Allgemeinen wird der Ersatz eines einzelnen Satelliten bei einer größeren Konstellation weniger kosten. Gleichzeitig erhöht die Verwendung von COTS-Produkten aber die Gefahr der Ausnutzung von Schwachstellen, da die Technologie standardisiert und auf dem Markt verfügbar und sie damit ein attraktiveres Angriffsziel ist.

Andererseits stellen Satelliten mit einzigartigen Nutzlasten das gegenteilige Szenario dar. Ein Herstellungsfehler kann das Ende der Mission bedeuten. Ein Verlust der Integrität entweder im Verhalten oder in den von der Nutzlast erzeugten Produkten kann ebenfalls eine erhebliche Einschränkung bzw. den Verlust der Mission bedeuten. In diesem Fall hat die Sicherung der Integrität der Daten an Bord eine höhere Priorität als die Frage, wie diese Daten der Einsatzleitung oder dem Kunden zur Verfügung gestellt werden können. Bei militärischen Missionen kann zusätzlich die geforderte Zeit für die Bereitstellung der Daten entscheidend für militärische Einsätze sein.

11.4 Stakeholder

Die Stakeholder einer Mission, d.h. AG, Kunde und Betreiber beeinflussen die Komplexität und organisatorischen Schnittstellen. Universitäre Forschung mit meist begrenztem Budget können flexible Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität haben.

Bei einem kommerziellen Betrieb werden spezifische Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit durch das Geschäftsmodell und die Kundenanforderungen diktiert. Die finanziellen Auswirkungen durch Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit können hier oft direkt in mögliche Bewältigungsmaßnahmen übersetzt werden oder als verbleibendes Restrisiko durch den Kunden akzeptiert werden.

Handelt es sich um staatliche oder staatengemeinschaftliche (z.B. EU-)Missionen spielen Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit eine erhebliche Rolle. Staatliche Missionen stellen Dienste für Bürger bereit oder werden zum Schutz von staatlichen bzw. öffentlichen Interessen betrieben. Dabei können besondere Sicherheitsanforderungen relevant sein, aber auch die Einschätzung von Risiken und deren mögliche Mitigation deutlich über die Maßnahmen von beispielsweise kommerziellen Missionen hinausgehen.

11.5 Zweck

Das Nutzerprofil und die Verwendung der Daten durch die Anwender spielen eine wichtige Rolle. Somit kann argumentiert werden, dass auch ein kommerzielles System, das von einem militärischen Nutzer verwendet wird, von böswilligen Akteuren der gleichen Klasse (wie staatlich finanzierte Gruppen) angegriffen wird. Jede Mission hat die Sicherheitsgrundlagen entsprechend dem Benutzerprofil und der Art des Dienstes festzulegen. Forschungsmissionen haben oftmals das Ziel, auf Basis der mit Instrumenten an Bord gesammelten Forschungsdaten neue Technologien zu testen oder Erkenntnisse zu gewinnen. Die Vertraulichkeit der Daten ist in der Regel zweitrangig. Die Verfügbarkeit der Instrumentendaten oder die mehrfache Erfassung derselben Daten stellt keine hinreichende Bedingung für die Mission dar, weshalb die Anforderung an die Verfügbarkeit im Vergleich zu anderen Missionszielen nicht hoch ist. Kommerzielle Missionen unterliegen oft sog. Service-Level-Vereinbarungen, und das Geschäftsmodell berücksichtigt auch Schäden durch Reputationsverluste.

Die Finanzierung von kommerziellen Missionen erfolgt jedoch ausschließlich oder überwiegend privat, so dass die Mittel für Investitionen begrenzt sind. Häufig verpflichtet sich der kommerzielle Betreiber zu einer

zertifizierbaren Basislinie, um ein Siegel zu haben, das einen Standard an Basisschutz für die Mission dokumentiert. Diese Basislinie und die Akkreditierung des Systems sind auch eine Voraussetzung für den Zugang zum staatlichen Nutzermarkt.

Zu den staatlichen Missionen zählen auch militärische Missionen, bei denen spezifische Fähigkeiten bereitgestellt werden. Diese Fähigkeiten werden dabei durch die Bereitstellung von bestimmten Satellitennutzlastfunktionen, unter Berücksichtigung des jeweiligen Anwendungsfalles, gewährleistet. Die bei diesen Prozessen entstehenden Informationen sind besonders schützenswert. In Abhängigkeit des jeweiligen Einstufungsgrades werden von staatlichen AG sowohl besondere technische als auch organisatorische Anforderungen an die Architektur, Hersteller und Betreiber von Bodenstationen gestellt.

11.6 Infrastruktur

In engem Zusammenhang mit dem Missionsziel sind die Eigentumsverhältnisse und der Betrieb der bodengebundenen Infrastruktur ein weiterer zu berücksichtigender Faktor für die Bestimmung des Schutzbedarfes.

Forschungsmissionen nutzen öffentliche Infrastrukturen für die Durchführung von Missionen. Hier findet Datenaustausch zwischen Universitäten und Forschungsinstituten statt. Der Betrieb wird durch öffentliche Einrichtungen und Personal durchgeführt. Es besteht außerdem die Möglichkeit, Bodenstationen zu mieten und über eine Verbindung über das Internet für eine Mission zu betreiben. In diesem Fall besitzt die Mission keine eigene Infrastruktur - mit Ausnahme der Missionskontrollsoftware, die auf einem lokalen IT-System, einer öffentlichen Cloud oder an einem anderen Ort bereitgestellt werden kann.

Im Gegensatz dazu verfügen Regierungsmissionen oft über eigene Infrastrukturen mit minimaler Exposition gegenüber offenen Netzen. Die Daten werden bei der Übertragung u.a. durch spezielle Sicherheitseinrichtungen geschützt. Der Betreiber des Bodensegments hat i.d.R. keinen Zugang zu den Nutzlastdaten: Entweder läuft der Download-Kanal außerhalb des Bodensegments des Betreibers oder der Datenzugang wird verschlüsselt.

Kommerzielle Missionen sind Missionen, die auf kosteneffiziente Bodensegmente angewiesen sind, um ihre Dienste wirtschaftlich bereitstellen zu können. Dies kann zu einer komplexen Anordnung von Partnern und Dienstleistern führen und umfasst dabei beispielsweise: Business-Support-System, Cloud-Ressourcen, Bodenstation als Dienst, Datenverarbeitung, Systemüberwachung, Satelliten- und Netzbetrieb, etc. Außerdem sind diese Missionen durch die hohe Anzahl von Interaktionen charakterisiert, von denen der Erfolg des endgültigen Dienstes abhängt. In diesem Fall müssen u.a. die Verträge mit den einzelnen Dienstleistern sorgfältig geprüft, die Zugriffsrechte der einzelnen Anbieter auf das Bodensystem begrenzt, die kritischen Funktionen des Systems im Rahmen des Plans zur Aufrechterhaltung des Geschäftsbetriebs berücksichtigt und ein ständiger Kompromiss zwischen Angriffsfläche, Gefährdung und Kosteneffizienz gefunden werden. Die Infrastruktur kann bei kritischen oder auf Gegenseitigkeit beruhenden Vermögenswerten Eigentum sein oder gemietet werden, was alle Cloud-Service-Modelle sowie Bodenstationsmodelle einschließt, sei es als Service oder als Eigentum für Backup oder Notfälle.

12 Schutzbedarfsfeststellung

Die Missionsmerkmale können in einem folgenden Schritt als Grundlage für die Feststellung des Schutzbedarfs der Bodenstation angewendet werden. Im Folgenden werden dazu Fallstudien bzw. Beispiele betrachtet, anhand derer der Einfluss der Missionsmerkmale auf den Schutzbedarf aufgezeigt und verdeutlicht werden soll.

Diese Faktoren für den Schutzbedarf können dem Benutzer helfen, seine Mission zu planen. Indem für jede der Säulen ausgewählt wird, auf welchem Teil des Spektrums sich das Missionsprofil befindet. Dadurch kann der Nutzer feststellen, welche Schutzprioritäten bestehen.

Grundlegend zur Festlegung des Schutzbedarfs sind die Schadensauswirkungen, die eine Verletzung der Schutzziele der Informationssicherheit hätten. Die folgende Tabelle stellt mögliche Schadensauswirkungen für die Schutzbedarfskategorien exemplarisch dar:

Tabelle 7: Schutzbedarfskategorien

Schutzbedarfskategorie	Schadensauswirkung
Normal	Die Schadensauswirkung für die Bodenstationen selbst oder für die Betreiber bzw. Hersteller der Bodenstationen und die Nutzer der Satellitendienste sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können den Betrieb der Bodenstation beträchtlich einschränken. Für die Betreiber oder die Hersteller können die Konsequenzen schwerwiegend sein.
Sehr hoch	Die Schadensauswirkungen können für den Betreiber oder den Hersteller ein existentiell bedrohliches, katastrophales Ausmaß erreichen. Sie können die Durchführung der Mission unmöglich machen.

12.1 Fallstudie 1: Cubesat

Die Schutzbedarfsfeststellung wird durch die Charakterisierung der geplanten Mission auf Basis der vorgestellten relevanten Missionsmerkmale (siehe Kapitel 11.1 - 11.6) unterstützt. Ein Cubesat mit einer oder mehreren Testnutzlasten von Forschungsinstituten und/oder Universitäten wäre beispielsweise charakterisiert durch:

Tabelle 8: Missionsmerkmale Cubesat

Missionstyp	Laufbahn	Konstellationsgröße	Zweck	Infrastruktur
Erdbeobachtung	LEO	Einzelner Satellit	Forschung	Öffentlich/Community Cloud

Die Schutzanforderungen wären daher wie folgt zu begründen:

Tabelle 9: Schutzbedarf Cubesat

Schutzziel	Forschungsdaten	Kontrolldaten	Design Dokumentation	Gesamt
Vertraulichkeit	Normal	Normal	Normal	Normal
Integrität	Sehr hoch	Hoch	Normal	Sehr hoch
Verfügbarkeit	Normal	Normal	Normal	Normal

Es ist entweder die Integrität der Nutzlastdaten oder des Technologiedemonstrators, welche den Schutzbedarf der Mission bestimmen. Es gibt nur eine Nutzlast dieser Art auf dem Cubesat, die Integration und Validierung ihrer Funktionalität, sowohl am Boden während der Testkampagne als auch im Flug, sind von großer Bedeutung für die Mission.

Der Erfolg der Mission hängt nur wenig vom Schutz der Vertraulichkeit der Daten ab. Auch eine zeitweilige Nichtverfügbarkeit des Bodensegments, des Kontakts zum Satelliten oder sogar der Nutzlastdaten, entweder vorübergehend oder auch wenn sie verloren gehen und wiederhergestellt werden müssen, gefährdet nicht das Ziel der Mission.

12.2 Fallstudie 2: GNSS

Eine andere Fallstudie für eine GNSS-bezogene Mission könnte der European Geostationary Navigation Overlay Service (EGNOS) sein, der mit einem so genannten Overlay-Dienst die Genauigkeit von PNT-Signalen verbessern und gleichzeitig eine Integritätsprüfung der Signalauthentizität und etwaiger Leistungsschwächen durchführt. Dabei werden GEO-Satelliten eingesetzt, um das Overlay-Signal auf der Grundlage von Messungen am Boden durch Referenzstationen auszustrahlen:

Tabelle 10: Missionsmerkmale GNSS

Missionstyp	Laufbahn	Konstellationsgröße	Zweck	Infrastruktur
GNSS	GEO	Mehrere	Staatlich	Staatlich

Das Ziel der Mission ist es, einen Dienst für mehrere kritische Marktsegmente wie Luftfahrt, Präzisionslandwirtschaft, Fahrzeugmanagement auf der Straße und Navigationsschiffe zu entwickeln. Die Anforderungen an diese Art von Diensten sind daher sehr hoch. Für die letztendliche Ermittlung des Schutzbedarfs muss eine gesonderte Betrachtung der verarbeiteten Daten erfolgen:

Tabelle 11: Schutzbedarf GNSS

Schutzziel	Navigationsdaten	Kontrolldaten	Design Dokumentation	Gesamt
Vertraulichkeit	Sehr hoch	Normal	Normal	Sehr hoch
Integrität	Hoch	Sehr hoch	Normal	Sehr hoch
Verfügbarkeit	Normal	Normal	Normal	Normal

Die Anforderungen an den Schutz des Bodensegments ergeben sich aus dem Nutzungsprofil des Dienstes. Deshalb ist diese kritische Infrastruktur hauptsächlich staatlich und unterliegt strengen Sicherheitsverfahren. Um die Verfügbarkeitsanforderungen zu erfüllen, gibt es redundante Anlagen am Boden, aber auch im Weltraum, d.h. mindestens zwei der vier Satelliten sind immer aktiv. Die Vertraulichkeit der Navigationsdaten wird als normal angesehen, da sie keinen Einfluss auf die Nutzer hat.

12.3 Fallstudie 3: Telekommunikationsdienste

Als drittes Beispiel kann eine kommerzielle Mission für Telekommunikationsdienste auf einer MEO-Umlaufbahn mit einer untereinander kommunizierenden Konstellation herangezogen werden:

Tabelle 12: Missionsmerkmale Telekommunikationsdienste

Missionstyp	Laufbahn	Konstellationsgröße	Zweck	Infrastruktur
Kommunikation	MEO	Mehrere	Kommerziell	IaaS

Der typische Aufbau für eine solche Mission besteht aus einem Bodenstationsnetz mit weltweiter Abdeckung und einer großen Anzahl von Kommunikationsgateways für die Nutzlast. Der kommerzielle

Betreiber unterliegt Dienstleistungsvereinbarungen, deren Verletzung zu Rufschädigung und Geldstrafen führen kann. Die kommerziellen Aspekte der Mission sind die treibende Kraft für das Sicherheitsdesign. Gleichzeitig kann das Profil des Kunden auch die Sicherheitsanforderungen definieren und beispielsweise festlegen, welche Art von Akkreditierung oder Konformität die Mission einhalten muss.

Diese Art von Mission kann potenziell viele Dienstanbieter umfassen, darunter Bodenstationen, öffentliche Clouds, Wetter- und Situationserkennungsdaten. Dies erfordert ein Risikomanagement in der Lieferkette und einen fundierten Risikomanagementprozess, um alle Risiken zu bewältigen, die sich aus einem System mit zahlreichen externen Schnittstellen und Beteiligten ergeben, denen das System ausgesetzt ist.

In entsprechend komplexen Anwendungsfällen bietet sich eine zusätzliche Betrachtung der verarbeiteten Daten bei der Schutzbedarfsfeststellung an. Dabei wurde der Schutzbedarf für die einzelnen verarbeiteten Informationen ermittelt und letztendlich kumuliert:

Tabelle 13: Schutzbedarf Telekommunikationsdienste

Schutzziel	Nutzerdaten	Benutzer-Metadaten	Kontrolldaten	Design Dokumentation	Gesamt
Vertraulichkeit	Sehr hoch	Hoch	Normal	Hoch	Sehr hoch
Integrität	Hoch	Sehr hoch	Sehr hoch	Hoch	Sehr hoch
Verfügbarkeit	Hoch	Normal	Hoch	Normal	Hoch

Diese Bewertung ist nur qualitativ und dient nur zur Orientierung. Sie zeigt, dass in einem Kommunikationsdienst die Vertraulichkeit der Nutzerdaten die höchste Priorität hat, gefolgt von der Integrität und Verfügbarkeit. Für den Systembetreiber hat die Integrität der Daten, die für die Steuerung des Systems zuständig sind, die höchste Priorität. Abrechnungen und Serviceanfragen beruhen auf Benutzer-Metadaten, daher muss die Integrität gewährleistet sein. Die sensible Dokumentation, die z.B. sicherheitsrelevant ist oder geistiges Eigentum enthält, muss vor Offenlegung oder Manipulationen geschützt werden.

Diese Art von Mission kann potenziell viele Dienstanbieter umfassen, darunter Bodenstationen, öffentliche Clouds, Wetter- und Situationserkennungsdaten. Dies erfordert ein Risikomanagement in der Lieferkette und einen fundierten Risikomanagementprozess, um alle Risiken zu bewältigen, die sich aus einem System mit zahlreichen externen Schnittstellen und Beteiligten ergeben, denen das System ausgesetzt ist.

13 Anwendungshinweise und Restrisiko

Im Falle des vorliegenden IT-Grundschutz-Profils sollte der Schutzbedarf jedes Prozesses missionsspezifisch und bezogen auf die jeweilige Lebensphase gründlich überprüft werden, da dieser bei den meisten Missionen über den angenommenen Schutzbedarf der Kategorie „normal“ hinausgehen kann und entsprechend höhere Anforderungen gestellt werden sollten. Das Profil dient als Umsetzungshilfe und muss individuell angepasst werden.

Auch bei der Umsetzung aller Anforderungen ist keine absolute 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 ggf. vertrauliche Informationen an Institutionen übertragen werden, auf deren Sicherheitsmanagement Hersteller und Betreiber nur beschränkt Einfluss nehmen können. Auch eigene Mitarbeiter können trotz Dienstanweisungen und Schulungen, absichtlich oder unbewusst, solche Informationen an Unbefugte weitergeben. Ferner beinhaltet der Bezug von Dienstleistungen über Dritte immer 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.