Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Resilienz im Weltraum – über die gesamte Lebensdauer des Satelliten

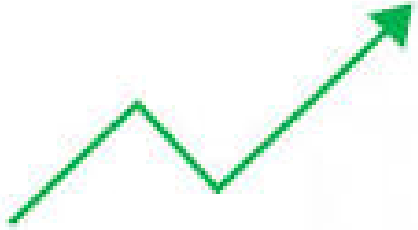
Omnisecure, Berlin

22.05.2023

Bedrohungslandschaft

„Boom im Weltraum“

- Wachsende Anzahl von Stakeholdern
- Wachsende Anzahl von Objekten
- Zunehmende Bedeutung und Abhängigkeit



Hohe Attraktivität für (Cyber-)Angriffe

- Geringe Einstiegshürde
- Überschaubarer Aufwand -> schwerer Schaden
- Fehlende Gemeinsame Mindestanforderungen an (Cyber-)Sicherheit

Stärkung der Cybersicherheit von Weltraumsystemen – gemeinsam im Team

Federal Office for Information Security

OHB DIGITAL

JADE UNIVERSITY OF APPLIED SCIENCES Wilhelmshaven Oldenburg Elsfleth

AIRBUS

secunet

DLR German Space Agency at DLR

Laufende Aktivitäten

Juni 2022 Veröffentlichung "***IT-Grundschutz-Profil*** *für Weltrauminfrastrukturen – Mindesabsicherung für den Satelliten über den gesamten Lebenszyklus*"

Herunterladen unter:

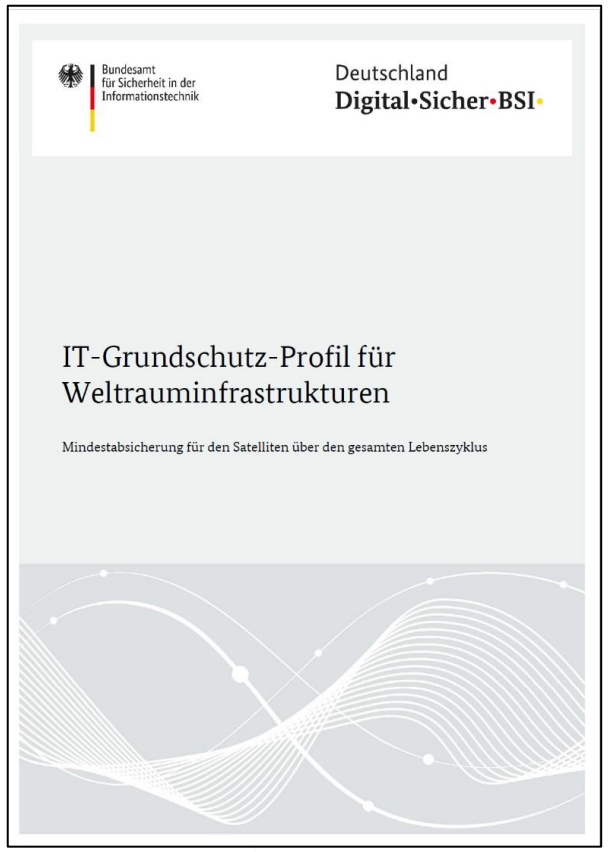
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Weltrauminfrastrukturen.html

Q2 2023 Veröffentlichung „***Technische Richtlinie*** – *Informationssicherheit für Weltraumsysteme"*

Q3 2023 Einrichtung ***Expertenkreis*** *Cybersicherheit Weltraum*

IT-Grundschutz Profil für Weltrauminfrastrukturen

Mindestabsicherung für den Satelliten über den gesamten Lebenszyklus

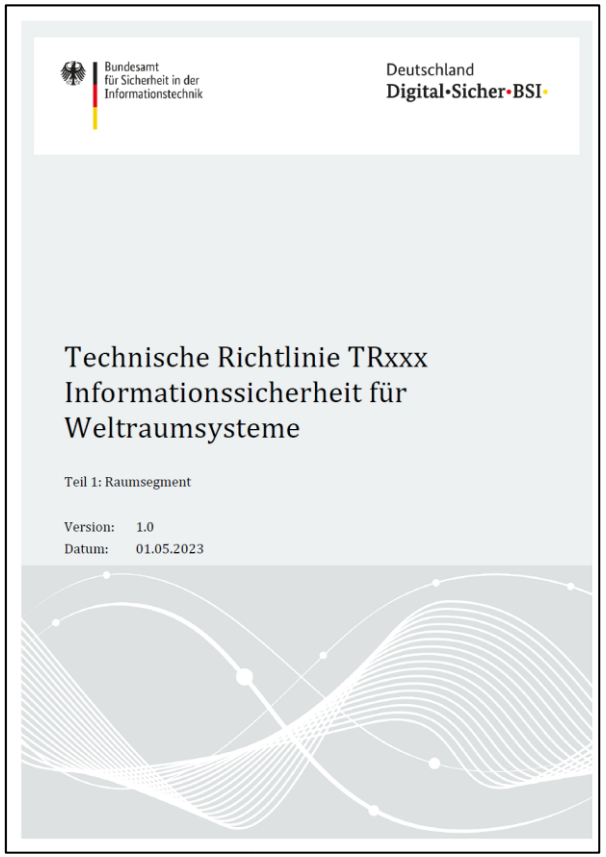


Ziele / Betrachtungsgegenstand:

- Informationssicherheit in allen Prozessen des Satelliten Lebenszyklus
- Empfehlungen für Mindestschutz des Satelliten (Satellitenintegration, Plattform, Nutzlast und Mission)
- Unterstützung für Informationssicherheitskonzept - "IT-Grundschutz", kompatibel mit ISO 27001

BSI-TR-xxxx Technische Richtlinie – Informationssicherheit für Weltraumsysteme

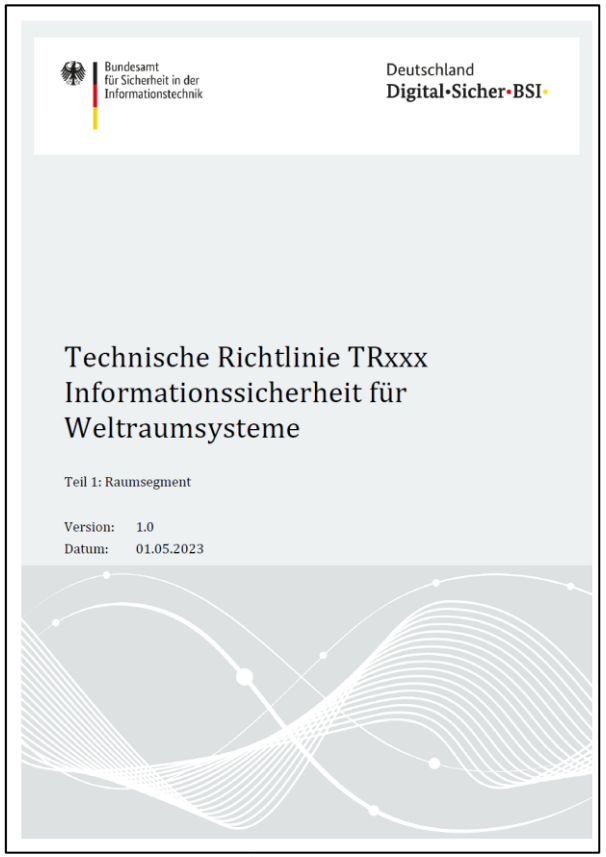
Veröffentlichung in Q2/2023



- Schutz von Informationen für hohen/sehr hohen Schutzbedarf
- Alle Lebensphasen des Systems
- Scope: Weltraumsystem - > Plattform

Zielgruppe & Ziele

Veröffentlichung in Q2/2023

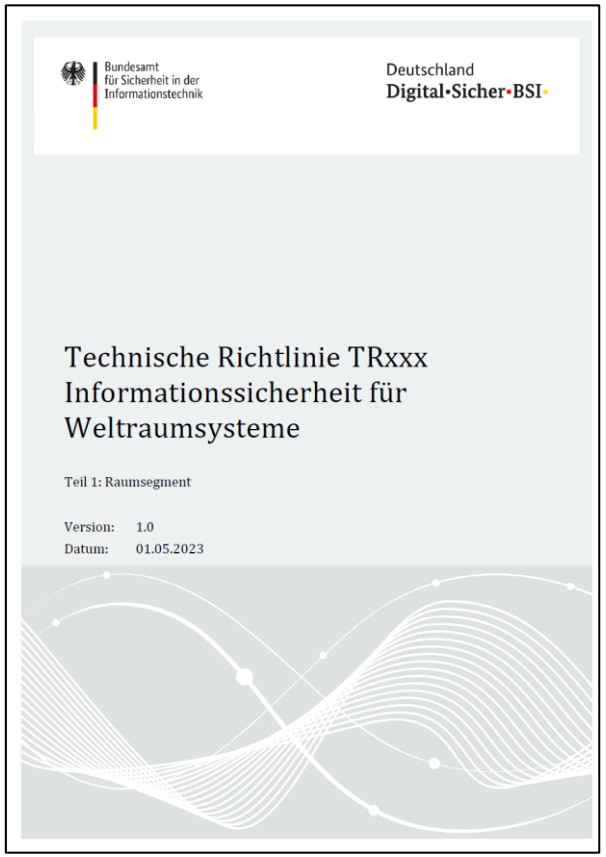


- Auftraggeber & Auftragnehmer
- Verantwortliche in Geschäftsprozessen
- externe Dienstleister

- Identifizieren von Risiken
- Definieren von Maßnahmen
- Formulierung von Anforderungen
- Anpassbar an Projekte

Anwendung

Veröffentlichung in Q2/2023



- Analyse je Geschäftsprozess
- Anwendungen den Geschäftsprozessen zugeordnet
- Gefährdungen identifiziert
- Bewältigungsmaßnahmen
  -> Maßnahmen qualitativ anpassen
  -> Requirements ableiten

Auszug aus Zuordnungstabelle

Veröffentlichung in Q2/2023

					BM27, BM31, BM32, BM33, BM37, BM39, BM40, BM48, BM49
G P02 Herstellung, G P03 Test, G P04 Transporte, G P05 Inbetriebnahme	A219	MGSE	G05	Physischer Zugriff durch Unbefugte	BM1, BM2, BM3, BM4, BM7, BM8, BM23, BM25, BM26, BM27, BM31, BM32, BM33, BM42, BM43, BM45, BM47
			G07	Logische Kompromittierung vernetzter Geräte	BM1, BM2, BM3, BM5, BM8, BM15, BM17, BM19, BM20, BM23, BM26, BM27, BM28, BM29, BM30, BM34, BM35, BM36, BM45, BM47, BM58
			G11	Schaden durch Umwelteinflüsse	BM9,BM10, BM11, BM12, BM13, BM15, BM16, BM22, BM37, BM38, BM39, BM41, BM48,
			G12	Zerstörung von Geräten und Medien	BM1, BM3, BM9, BM10, BM11, BM13, BM21, BM26, BM27, BM31, BM32, BM33, BM37, BM38, BM39, BM40, BM41, BM42, BM48,
			G13	Ausfall der Stromversorgung	BM12, BM15, BM21, BM22, BM33, BM40, BM48, BM49

Ausblick

Weitere Partner aus ACS für Feedback und Austausch mit der Arbeitsgruppe willkommen.

Bitte kontaktieren Sie uns:

Referat Sichere IT-Systeme für Luft- und Raumfahrt

itcssa@bsi.bund.de