

# Mehr Resilienz für Weltraumsysteme im Kontext europäischer Regularien

Interaktiver Workshop des ACS-Expertenkreises für Cybersicherheit im Weltraum



Bundesamt  
für Sicherheit in der  
Informationstechnik

Omnisecure, Berlin, 20. Januar 2026

# Expertenkreis Cybersicherheit im Weltraum

## Daten:

- Gegründet: November 2023
- Aktuell ca. 75 Mitglieder

## Ziele:

- Austausch zwischen Behörden, Industrie und Forschungseinrichtungen in Deutschland zum Thema Cybersicherheit Weltraum
- Sensibilisierung für die Dringlichkeit des Themas
- Aufbau eines gemeinsamen Verständnisses von Sicherheitsanforderungen
- Einbringen national abgestimmter Positionen in internationale Standards

## Kontakt und Publikationen:

Website [Expertenkreis Cybersicherheit im Weltraum](#)



# Gemeinsam die Cybersicherheit von Weltraumsystemen stärken

**infodas**  
connect more. be secure.

**OHB**

**CYBERINTELLIGENCE**  
Institute

**DLA PIPER**



**Fraunhofer**  
SIT

**Condify**

**SANCTUARY**  
The Embedded Security Experts

**TUVIT**

Allianz für  
Cyber-Sicherheit



**Universität München**  
der Bundeswehr

**CGI**

**iABG**

**DLR** Gesellschaft für  
Raumfahrtanwendungen

**AIRBUS**



**Munich Center for  
Space Communications**

**cyberagentur**



Federal Office  
for Information Security

**BHO**  
LEGAL

**TELESPAZIO**  
a LEONARDO and THALES company

**JADE** UNIVERSITY  
OF APPLIED SCIENCES  
Wilhelmshaven Oldenburg Emden

**spaceopal**  
a DLR GfR and Telespazio company

**Bundesamt**  
für Bevölkerungsschutz  
und Katastrophenhilfe

# Schwerpunkte Expertenkreis



## PG-D Identifizierung von Sicherheitsanforderungen

- Risiko-orientierter Ansatz über gesamten Lebenszyklus
- IT-Grundschutz-Profile, TRs



## PG-Z Zukunftstechnologien / Space 4.0

- Technologien, Entwicklungen, Geschäftsprozesse, Stakeholder



## PG-N Nutzbarkeit

- Sensibilisierung, Motivation für CS in WR-Systemen
- Anwendung der Dokumente in Projekten



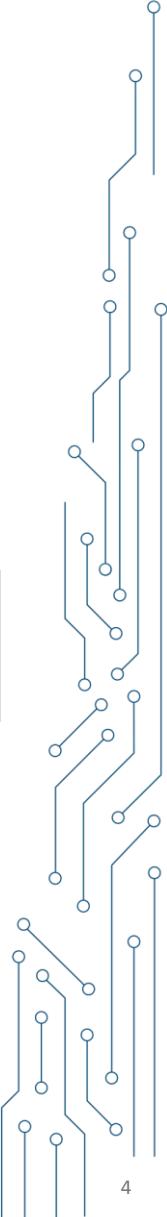
## PG-I Internationales, Standardisierung

- Unterstützung für und Austausch mit Gremien
- Einbringen in internationale Standards und Reviews

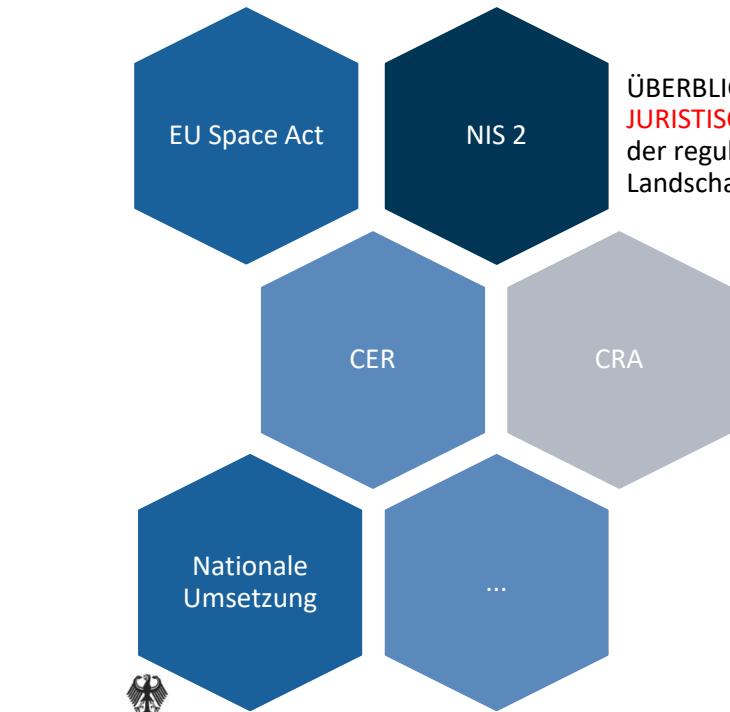


## PG-R Regulierung

- Mehrstufiges Zertifizierungsschema
- EU Space Act, NIS 2, CRA



# Was passiert heute?



Best Practices – Erhöhung der Rechtssicherheit und operativen Robustheit durch Standards



# Europäisches Cybersicherheitsrecht – Überblick und juristische Analyse

## Wer/was ist erfasst?

(Besonders) wichtige  
Einrichtungen

Kritische  
Einrichtungen

Betreiber von WR-Missionen,  
Anbieter von WR-basierten Daten

Hersteller (u.a.) von  
Produkten mit digitalen Elementen

NIS 2

CER

EU Space Act

CRA

BSIG

KRITIS-DachG

Europäisches System für Cybersicherheitszertifizierungen, inkl. EUCC

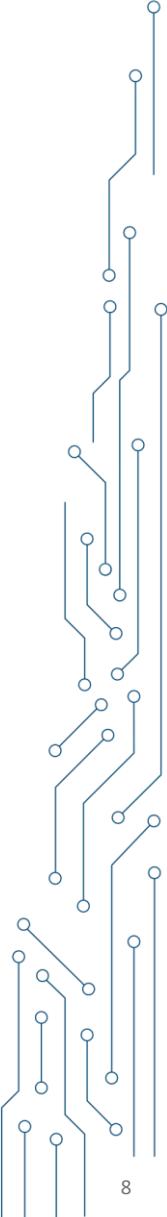


# NIS 2 & BSIG – Cybersicherheits-Risikomanagement

## Mindestanforderungen

### Art. 21 Abs. 2 NIS-2-Richtlinie <> § 30 Abs. 2 BSIG

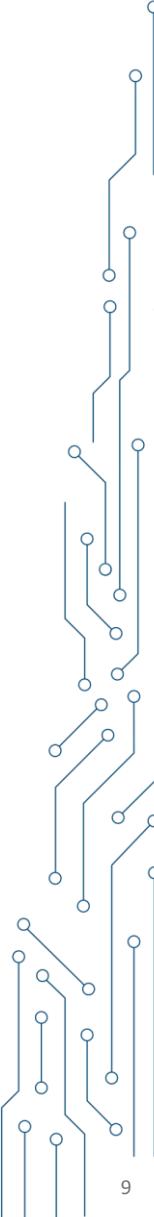
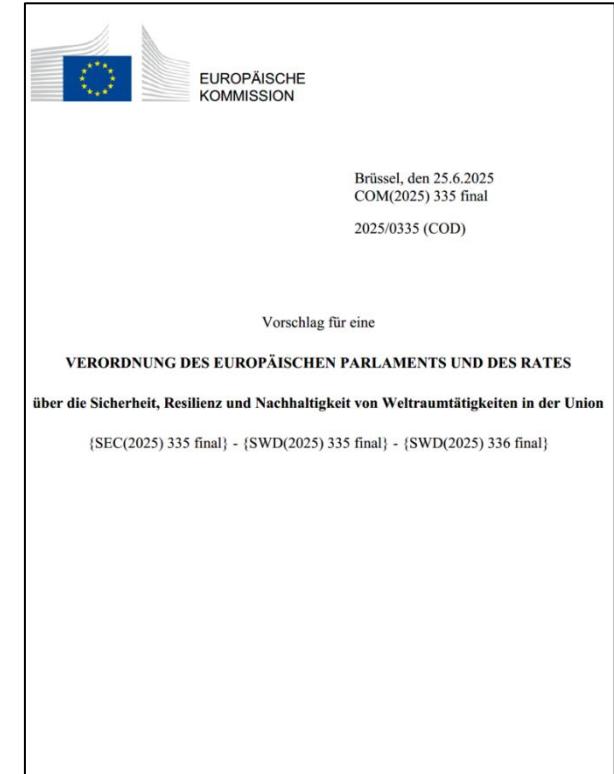
1. Risikoanalyse
2. Bewältigung von Sicherheitsvorfällen
3. BCM und Krisenmanagement
4. Lieferkettensicherheit
5. Schwachstellenmanagement
6. Wirksamkeitsbewertungen
7. Cyberhygiene und Schulungen
8. Kryptografie und Verschlüsselung
9. Personalsicherheit, Zugriffskontrolle und Anlagenmanagement
10. MFA, Authentifizierung, gesicherte Kommunikation



# EU Space Act (Entwurf)

**Entwurf vom 25. Juni 2025: Eigene Anforderungen an Resilienz der Weltrauminfrastruktur und Risikomanagement für Cybersicherheit gemäß Artikel 75-95 EUSA**

- Risikomanagement einschließlich Risikobewertungen
- Leitungsverantwortung, Personalsicherheit
- Zugangsrechte
- Prävention und Schutz, auch vor Sicherheitsvorfällen
- Kryptografie und Verschlüsselung
- BCM einschließlich Backup-Management
- Prüfprogramm für die Netz- und Informationssysteme, Pen Tests
- Umgang mit Sicherheitsvorfällen, Krisenmanagement
- Meldung erheblicher Sicherheitsvorfälle
- Schulungen
- Lieferkettensicherheit



## EU Space Act (Entwurf)

Entwurf vom 25. Juni 2025: Verhältnis zu NIS-2-Richtlinie und CER-Richtlinie

## Verhältnis NIS-2-Richtlinie und EU Space Act:

Für *wichtige und wesentliche Einrichtungen* gemäß NIS-2-Richtlinie gilt:

- >> Für Risikomanagementmaßnahmen: EU Space Act ist speziellerer Rechtstakt (Art. 75 Abs. 1 EUSA)  
>> Im Übrigen ist eine Anwendung der NIS-2-Richtlinie aber nicht ausgeschlossen

## Verhältnis CER-Richtlinie und EU Space Act:

Für *kritische Einrichtungen* gemäß CER-Richtlinie gilt:

- >> CER-Richtlinie findet neben dem EU Space Act Anwendung
  - >> Auch nationales Umsetzungsrecht ist neben dem EU Space Act anwendbar:  
Bsp.: Systeme zur Angriffserkennung (§ 31 Abs. 2 BStG) für Betreiber kritischer Anlagen

# EU Space Act (Entwurf)

## Entwurf vom 5. Dezember 2025: Art. 75 und 75a EUSA

- Verhältnis zu NIS-2-Richtlinie (Art. 75 Abs. 1 EUSA) – Parallelität
- Verhältnis zu CER-Richtlinie (Art. 75 Abs. 2 EUSA) – Parallelität
- Cybersicherheitsanforderungen für *wichtige und wesentliche Einrichtungen* gemäß NIS-2-RL:
  - Durchführungsrechtsakt der Kommission
  - Mindestens Anforderungen gemäß Art. 21 Abs. 2 NIS-2-Richtlinie
    - >> Auf den ersten Blick: Synergie / Vereinheitlichung der Cybersicherheitsanforderungen
    - >> Aber: Inhalt des KOM-Rechtsakts entscheidend, kann auch darüber hinausgehen
- Cybersicherheitsanforderungen für *sonstige* Betreiber von Weltraummissionen oder Anbieter von weltraumbasierten Daten, inkl. *Drittlandsbetreiber und -anbieter, internationale Organisationen* und *EU-Betreiber von unionseigenen Ressourcen* (Art. 75a):
  - Spezifische Cybersicherheits-Anforderungen (Art. 75a Abs. 4 EUSA)
  - Anforderungen ähneln jedoch aktuell stark den Anforderungen an NIS-2-Richtlinie
    - >> Unklar, warum Anforderungen strukturell anders sein sollen, sich dann aber inhaltlich doch annähern (ohne identisch zu sein)

# Cyberresilienz-Verordnung (CRA)

## Einheitlicher EU-Rechtsrahmen für Cybersicherheitsanforderungen an Produkte mit digitalen Elementen (PDE)

- CRA ist in Kraft, produktbezogene Cybersicherheits-Anforderungen gelten aber erst ab dem **11. Dezember 2027**
- PDE sind in verschiedene **Klassen** eingeteilt:
  - **Wichtige PDE** (z.B. Identitätsmanagement, Firewalls)
  - **Kritische PDE** (z.B. Hardwaregeräte mit Sicherheitsboxen)
- CRA gilt für **Hersteller**, Distributoren, Importeure, Händler  
>> Hauptverantwortung während gesamten Lebenszyklus beim Hersteller.
- Lieferanten und Unterlieferanten: indirekt betroffen, da der Hersteller zur **Lieferkettensicherheit** verpflichtet ist.



## Ausgewählte Cybersicherheitsanforderungen an die Eigenschaften von PDE und Behandlung von Schwachstellen:

- Sichere Standardkonfiguration (*security by default*)
- Schwachstellenmanagement einschließlich regelmäßige Sicherheitsaktualisierungen
- Zugriffskontrolle (IAM)
- Verschlüsselung
- Datenintegrität, Datenminimierung
- Verfügbarkeit wesentlicher Funktionen, Minimierung negativer Auswirkungen auf andere Geräte
- Möglichst geringe Angriffsflächen (*security by design*)

# Mapping gesetzlicher Cybersicherheits-Anforderungen

Anforderung	EUSA (i.d.F.v. 25.6.2025) (Art. 76-95)	BSIG (i.d.F.v. 5.12.2025) (§§ 28-42)	CRA (Art. 13 i.V.m. Anhang I)
<b>Risikomanagementsystem (ISMS / RMS)</b>	Verpflichtung zur Einrichtung, Umsetzung und Aufrechterhaltung eines risikobasierten Managementsystems über den gesamten Missions- und Lebenszyklus hinweg (Art. 76 Abs. 1, 5, 6)	Verpflichtung zu risikobasierten Maßnahmen nach dem Stand der Technik (§ 30 Abs. 1 u. 2); besondere Pflichten für KRITIS (§ 31)	Verpflichtung zur Durchführung einer Cybersicherheits-Risikobewertung als Grundlage aller Produktanforderungen (Art. 13 Abs. 2)
<b>Governance / Verantwortung der Leitung</b>	Leitungsorgan haftet für Umsetzung und Überwachung der Maßnahmen (Art. 77 Abs. 1)	Geschäftsleitung ist für Umsetzung und Überwachung verantwortlich (§ 38 Abs. 1)	Hersteller trägt Gesamtverantwortung für Konformität (Art. 13 Abs. 1)
<b>Identitäts- und Zugangsmanagement</b>	Verpflichtung zu IAM-Protokollen (Art. 81 Abs. 1)	Zugriffskontrolle und MFA verpflichtend (§ 30 Abs. 2 Nr. 10, 11)	Schutz vor unbefugtem Zugriff verpflichtend (Anhang I Nr. 1 d)
<b>Kryptographie und Schlüsselmanagement</b>	Detaillierte Vorgaben inkl. Ende-zu-Ende-Authentifizierung (Art. 85)	Pflicht zu Konzepten für kryptographische Verfahren (§ 30 Abs. 2 Nr. 8)	Verschlüsselung als zentrale Sicherheitsmaßnahme (Anhang I Nr. 1 e)
<b>Backup und Recovery</b>	Pflicht zu Backup- und Wiederherstellungsstrategien (Art. 86)	Pflicht zu Backup und Notfallwiederherstellung (§ 30 Abs. 2 Nr. 4)	Sicherstellung der Verfügbarkeit nach Vorfällen (Anhang I Nr. 1 h)
<b>Business Continuity / Krisenmanagement</b>	Verpflichtende Reaktions- und Wiederherstellungspläne (Art. 87)	Bestandteil der Risikomanagementmaßnahmen (§ 30 Abs. 2 Nr. 3)	Mittelbar durch Verfügbarkeits- und Updatepflichten sowie gemäß Anhang I Nr. 1 h)
<b>Tests und Prüfungen</b>	Verpflichtendes Prüf- und Testprogramm (Art. 88)	Nachweis- und Prüfpflichten (§§ 35-37)	Regelmäßige Sicherheitsüberprüfungen (Anhang I Nr. 2)
<b>Schulungen und Awareness</b>	Verpflichtende Schulungen (Art. 89)	Schulungs- und Sensibilisierungspflichten (§ 30 Abs. 2 Nr. 8)	Nicht ausdrücklich
<b>Incident- und Schwachstellenmanagement</b>	Meldepflichten und Incident-Handling-Prozesse (Art. 78 Abs. 1 c) und Art. 91, 93)	Melde-, Nachweis- und Informationspflichten (§ 32)	Umfassendes Vulnerability-Management inkl. SBOM (Art. 14, Anhang I Teil II Ziffer 1)
<b>Lieferketten-Risikomanagement</b>	Verpflichtender Lieferketten-Risikomanagement-Rahmen (Art. 92, Anhang VII Nr. 6)	Pflicht zur Berücksichtigung der Lieferkette (§ 30 Abs. 2 Nr. 4)	Hersteller haftet für Cybersicherheit entlang der Lieferkette (CRA fokussiert auf SBOM)

# Europäisches System für Cybersicherheitszertifizierung

Rechtsakt zur Gründung der Europäischen Cybersicherheitsagentur (ENISA) stellt Grundlage dar für Einführung europäischer Schemata für Cybersicherheitszertifizierung

- **EUCC: EU-Schema auf der Grundlage Gemeinsamer Kriterien (Common Criteria)**, gilt für Produkte der Informations- und Kommunikationstechnik
- Gegenstand einer Zertifizierung können sein:
  - IKT-Produkt
  - IKT-Dienst
  - IKT-Prozess
  - verwalteter Sicherheitsdienst
- Die Zertifizierung erfolgt **grundsätzlich auf freiwilliger Basis**.
- Soweit IKT-Produkte, IKT-Dienste, IKT-Prozesse, und/oder verwaltete Sicherheitsdienste zertifiziert wurden, gilt die **Vermutung**, dass diese den Anforderungen des angewandten Schemas, d.h. des EUCC, genügen.



## Mögliche Synergien:

- >> In Art. 27 CRA, Art. 24 NIS-2-Richtlinie, und Art. 85 Abs. 4 EUSA ist vorgesehen, Zertifizierung und Erfüllung rechtlicher Anforderungen zu verknüpfen (vorbehaltlich nationaler Regelungen und KOM-Rechtsakte).
- >> § 30 Abs. 6 BSIG: (Besonders) wichtige Einrichtungen dürfen bestimmte IKT-Produkte, -Dienste und Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata verfügen.
- >> Einrichtungs-bezogene Cybersicherheitsanforderungen sind damit aber nicht erfasst.

## Bisherige Ergebnisse in Arbeitsthesen

1. EU Space Act (Erster Entwurf der Kommission) enthält bislang die detailliertesten Resilienz- und Cybersicherheitsanforderungen.
2. Spezifische Anforderungen sind grundsätzlich gerechtfertigt durch Besonderheiten im Sektor Weltraum.
3. Mindestanforderungen durch NIS-2-Richtlinie führen tendenziell zu unterschiedlichen Schutzniveaus in den EU-Mitgliedstaaten.
4. National höhere Anforderungen dienen der Cybersicherheit, sind aber potenziell negativ für die wirtschaftlichen Akteure in diesen Mitgliedstaaten.
5. Einheitlicher, sektorspezifischer Rechtsrahmen für Cybersicherheit im Weltraumbereich wäre daher sinnvoll.
6. Ermöglichung entweder durch eigenständigen EU-Rechtsakt und spezifischen Durchführungsrechtsakten (Erster Vorschlag EUSA) ODER Nutzung europäischer Standards, die die technischen und organisatorischen Maßnahmen enthalten und die Vermutung aufstellen, dass bei deren Erfüllung auch die gesetzlichen Anforderungen (EUSA, NIS 2, BSIG, CRA) erfüllt sind.
7. EU-Schemata mit einheitlichen Cybersicherheitsanforderungen können helfen, die teils mehrfach existierenden gesetzlichen Anforderungen zu erfüllen und die Erfüllung durch Zertifizierung nachzuweisen; hierfür bedarf es geeigneter Schemata und entsprechender KOM-Rechtsakte / nationaler Rechtsakte, die diese anerkennen und die Erfüllungsvermutung statuieren.



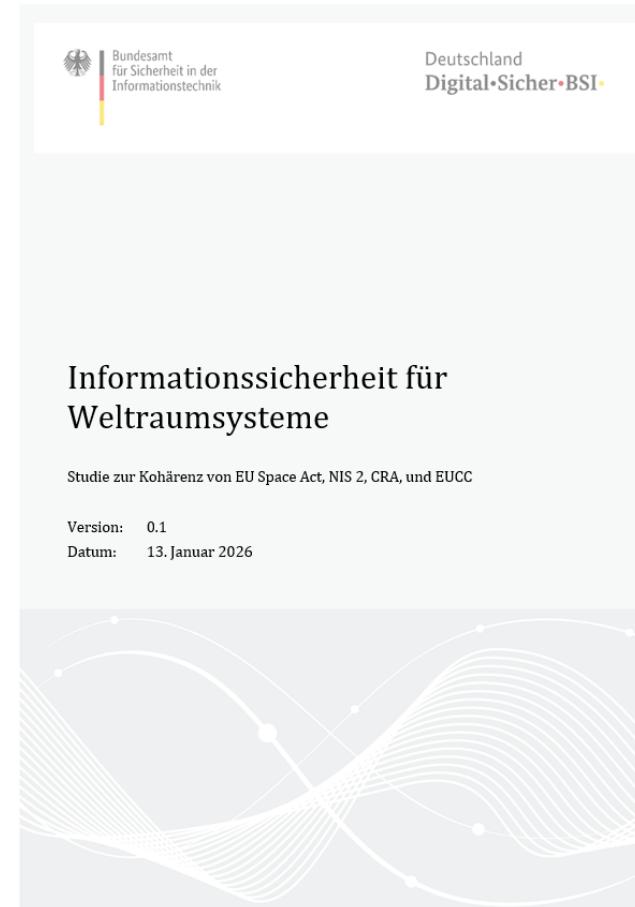
*Alternativ oder ergänzend gibt es schon heute **Technische Richtlinien** und **Schutzprofile** des BSI, die die aktuelle Lücke füllen können.*

# HOW TO – Operative Nutzung der BSI-Dokumente

## Anleitung zur effizienten Umsetzung gesetzlicher / regulatorischer Anforderungen

### Mapping der einzelnen Anforderungen in den BSI-Dokumenten mit den gesetzlichen und regulatorischen Anforderungen

- **Anlagen** zur Studie
- Aktuell im **Entwurfsstadium**
- Zur **Veröffentlichung** geplant, abrufbar über Website  
Expertenkreis Cybersicherheit im Weltraum (Link via QR Code)



## IT-Grundschutz-Profil für Weltrauminfrastrukturen

Mindestabsicherung für den Satelliten über den gesamten Lebenszyklus

## Technische Richtlinie BSI TR-03184 Informationssicherheit für Weltraumsysteme

Teil 1: Raumsegment

Version: 1.0  
Datum: 31.05.2023

# IT-Grundschutz-Profil und Technische Richtlinie

Dokumente direkt von bsi.de:



**Frage:**  
Können die Dokumente zur  
Rechtsicherheit beitragen?

## IT-Grundschutz-Profil für Weltraumsysteme

Teil 2: Bodensegment - Mindestabsicherung über den gesamten Lebenszyklus

## Technische Richtlinie BSI TR-03184-2 Informationssicherheit für Weltraumsysteme

Teil 2: Bodensegment

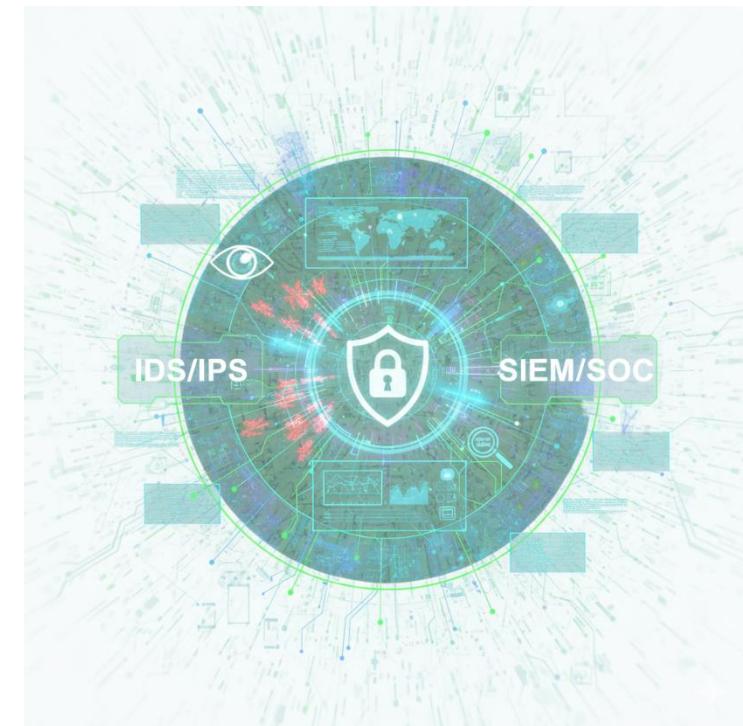
Version: 1.0  
Datum: 12.05.2025

# Vom abstrakten Paragraphen zum konkreten Handeln

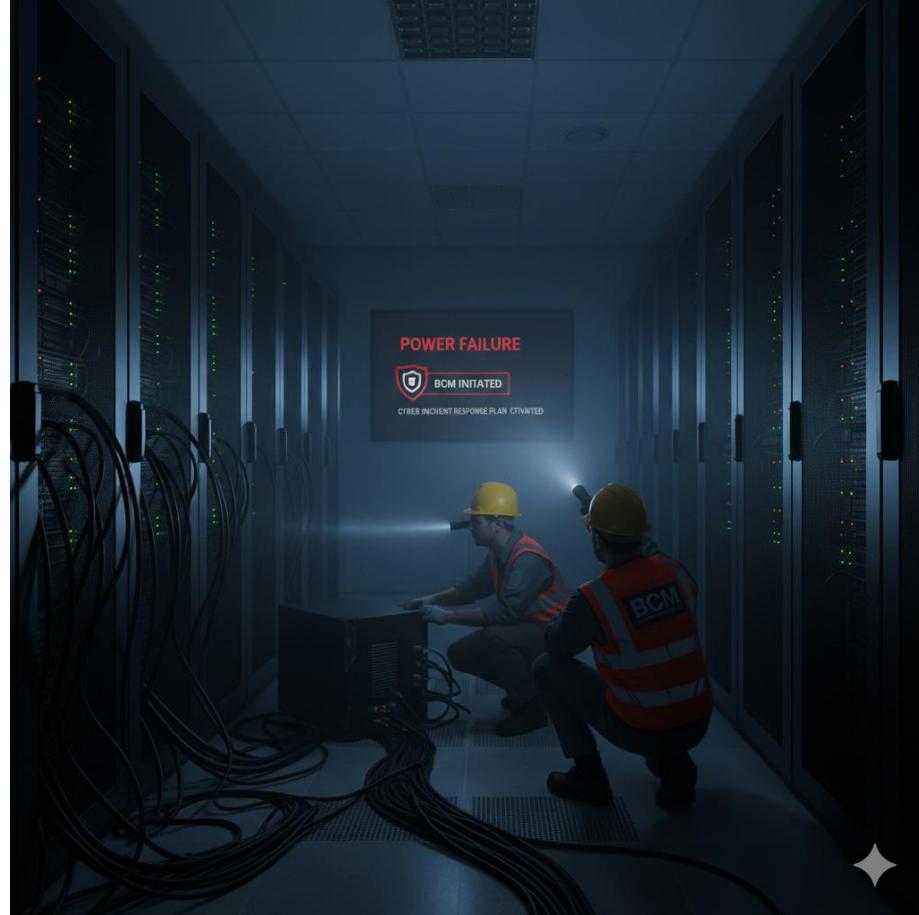
Gesetzliche Anforderung (BSIG)	TR-03184-1/2 Maßnahmen - Profile	Konformität
Anforderungen an besonders wichtige und wichtige Einrichtungen: § 30 Abs. 1 Nr. 1: Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	Kap.6 Risikobehandlung von Gefährdungen, Kap. 5 (Schutzbedarfsfeststellung), Kap. 10.4 Risikomanagement	[++) Erfüllt
§ 30 Abs. 1 Nr. 2: Maßnahmen zur Bewältigung von Sicherheitsvorfällen	BM8, BM19, BM59, DER.1, DER.2.1	[+] Erfüllt
§ 30 Abs. 1 Nr. 3: Aufrechterhaltung des Betriebs, wie Backup-Management	<b>§ 30 Abs. 1 Nr. 2: Maßnahmen zur Bewältigung von Sicherheitsvorfällen</b>	[++) Erfüllt*
§ 30 Abs. 1 Nr. 4: Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern	<b>§ 30 Abs. 1 Nr. 3: Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement</b>	[+] Teilweise erfüllt
§ 30 Abs. 1 Nr. 5: Sicherheitsmaßnahmen bei Erhaltung und Wartung von informationstechnischen Systemen, einschließlich Management und Offenlegung von Risikomanagementmaßnahmen im Bereich der Informationstechnik	<b>§ 30 Abs. 1 Nr. 4: Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern</b>	[++) Erfüllt
§ 30 Abs. 2 Nr. 7: Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik	<b>§ 30 Abs. 1 Nr. 5: Sicherheitsmaßnahmen bei Erhaltung und Wartung von informationstechnischen Systemen, einschließlich Management und Offenlegung von Risikomanagementmaßnahmen im Bereich der Informationstechnik</b>	[++) Erfüllt
§ 30 Abs. 1 Nr. 8: Konzepte und Prozesse für den kryptographischen Verfahren	<b>§ 30 Abs. 1 Nr. 6: Konzepte und Verfahren zur Bewältigung von Sicherheitsvorfällen</b>	[++) Erfüllt
§ 30 Abs. 1 Nr. 9: Erstellung von Konzepten für die Zugriffskontrolle und für die Verwaltung von Benutzern und -Prozessen	<b>§ 30 Abs. 1 Nr. 7: Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik</b>	[++) Erfüllt
§ 30 Abs. 1 Nr. 10: Verwendung von Lösungen zur Authentifizierung oder kontinuierlichen Authentifizierung von Benutzern, einschließlich Sprach-, Video- und Textkommunikation sowie gezielte Notfallkommunikationssysteme innerhalb der Einrichtung	<b>§ 30 Abs. 1 Nr. 8: Konzepte und Prozesse für den kryptographischen Verfahren</b>	[++) Erfüllt
Zusätzliche Anforderungen an Betreiber kritischer Anlagen: § 31 Abs. 2: Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.	BM45, ORP.4 BM59	[o]*

# Vorfallbehandlung (§ 30 Abs. 1 Nr. 2)

- **Detektion: BM8 (IDS/IPS Systeme)** Einsatz von Host- oder Netzwerk-Intrusion Detection/ Prevention Systemen (signaturbasiert oder Anomalie basiert)
- **Analyse: BM19 (Regelmäßiges Prüfen von Logginginformationen/-protokollen )**  
Implementierung und Umsetzung der entsprechenden Prozesse zu Art und Häufigkeit des Auditings sowie toolgestützte Überprüfung und Auswertung von Logginginformationen im Rahmen des Auditings
- **Reaktion: BM59 (SIEM/SOC)**  
Zentrales Incident Management & Response (SIEM/SOC) angelehnt an IT-Grundschutz DER.1 gemäß BM59.



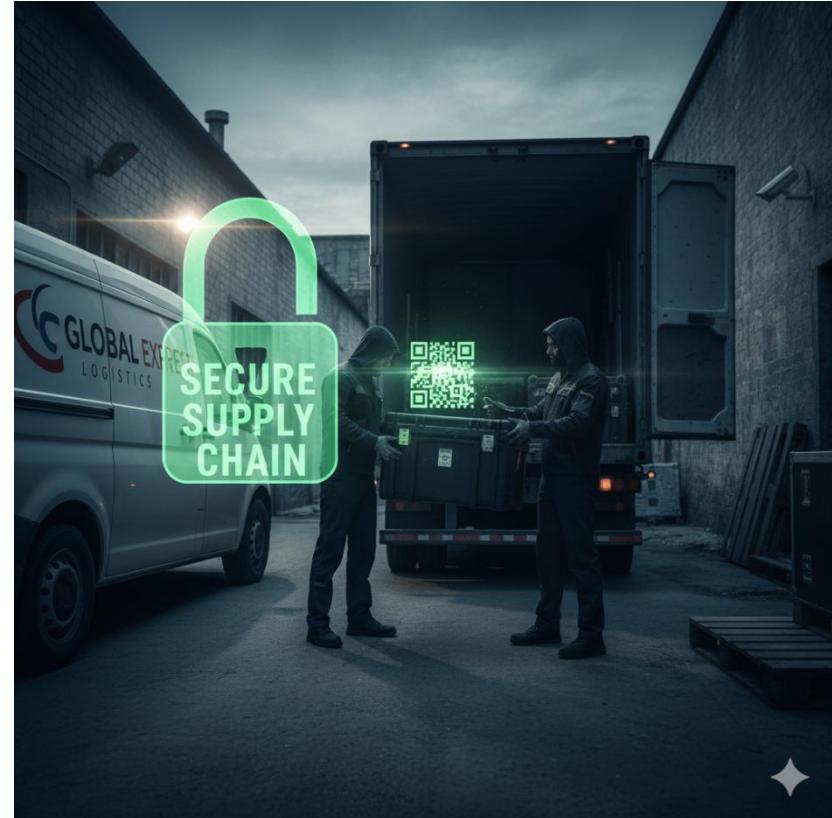
# Geschäftskontinuität (§ 30 Abs. 1 Nr. 3)



- **Resilienz: BM16 (Redundanzsystem)**  
Sicherstellung der Verfügbarkeit und Funktionsfähigkeit z.B. auch durch Wiederherstellung von Datenbeständen
- **Planung: BM22 (Notfallkonzept)**  
Beachtung des BSI 200-4 Standards; gelebte Umsetzung des Konzepts z.B. durch sensibilisieren des Personals
- **Ziel:** Einhaltung definierter Wiederherstellungszeiten für den Betrieb.

# Lieferkettensicherheit (§ 30 Abs. 1 Nr. 4)

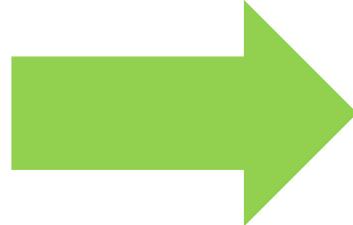
- **Produktprüfung: BM5 (Software-Integritätscheck)**  
Sicherstellung der Integrität durch  
technische Maßnahmen (z.B. Hashsumme)  
und organisatorische Maßnahmen (z.B.  
versiegelte Briefe, persönliche Übergabe)  
sowie Auditierung der Zulieferer
- **Lieferantenprüfung: BM36  
(Softwarelieferanten prüfen)**  
Überprüfung der Software-Lieferkette z.B.  
VS-Belehrung
- **Logistik: BM32 (Vertrauenswürdiger Transport)**  
Sicherstellung vertrauenswürdiger  
Transporte durch Sicherheitsüberprüfungen  
des Personals



# Zusammenfassung – Vom Paragraphen zum konkreten Handeln

## Herausforderung:

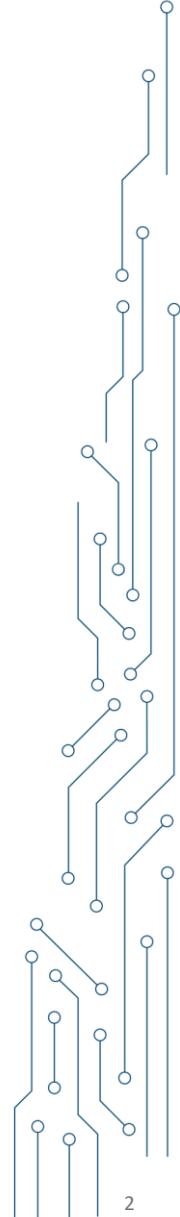
- „vage Gesetzestexte“
- „Komplexität“
- „Unklare Prüfungsziele“



## Lösung?

- Fundament der Compliance
- Schutzbedarfsfeststellung als Hebel
- Präzision durch Profil und TR
- „Audit-Readiness“

→ Die Profile und TR machen Cybersicherheit im Weltraumsektor messbar und prüfbar



# Fragen?

# Kontakt

**Dr. Holger A. Kastler**

[holger.kastler@dlapiper.com](mailto:holger.kastler@dlapiper.com)

DLA Piper

Maximilianstr. 2

80539 München



Bundesamt  
für Sicherheit in der  
Informationstechnik

**Sascha Fankhänel**

[sascha.fankhaenel@jade-hs.de](mailto:sascha.fankhaenel@jade-hs.de)

Jade Hochschule

Friedrich-Paffrath-Str. 101

26386 Wilhelmshaven



**Dr. Johanna Niecknig**

[johanna.niecknig@bsi.bund.de](mailto:johanna.niecknig@bsi.bund.de)

[xprt-space@bsi.bund.de](mailto:xprt-space@bsi.bund.de)

Bundesamt für Sicherheit in der  
Informationstechnik (BSI)  
Godesberger Allee 87

53175 Bonn

[www.bsi.bund.de](http://www.bsi.bund.de)

Follow us:



Bild: © AdobeStock/Nirut