Cybersicherheit im Straßenverkehr

Bundesamt
für Sicherheit in der
Informationstechnik

Überblick

- Cybersicherheit der Ladeinfrastruktur
- Cybersicherheit vernetzter Fahrzeuge
- Regulierung

Unsere Stakeholder

Staat

Wirtschaft

Gesellschaft

Wissenschaft

Prävention

Detektion

Reaktion

- Übernahme technischer Schutzmaßnahmen
- Nationales IT-Lagezentrum
- Technische Unterstützung und Dienstleistungen
- CERT-Bund und MIRTs
- Beratung und Service-Center
- Kooperation
- Allianz für Cybersicherheit
- UP KRITIS
- Begleitung in der Aus- und Fortbildung
- Technische Richtlinien
- Zertifizierung
- IT-Sicherheitskennzeichen

Bundesamt für Sicherheit in der Informationstechnik

Gründung

01. Januar 1991

Bundesministerium des Innern und für Heimat

Bundesamt für Sicherheit in der Informationstechnik

Stellen 2025

1.791

Stellenbesetzungsquote: 94 %

***ohne Zuläufe**

64

Unbefristete Mitarbeitende im Zulauf

Stand: 31.12.2025

36 %* **Frauen**

64 % **Männer**

*Anteil in Leitungsfunktion: 28 %

Stand: 31.12.2025

379 Mio. Euro

Haushalt 2026

Cybersicherheit der Ladeinfrastruktur

Gefühlte Cyber-Bedrohungslage

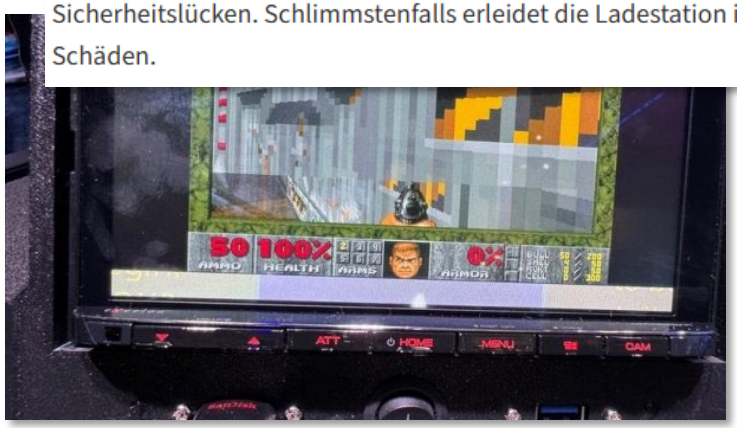
Schwachstellen in Ladestationen

Electrify America Charging Stations Vulnerable To Hacking

Thankfully, the person who discovered and shared the bug didn't have bad intentions, but EA isn't happy about the access.

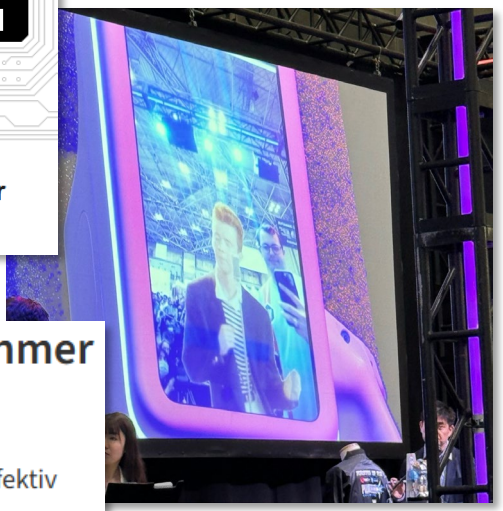
E-Auto gratis beim Nachbarn laden: Schwachstellen in Level-2-Wallboxen entdeckt

Sicherheitsforscher fanden in drei Wallboxen für Privathaushalte reichlich Sicherheitslücken. Schlimmstenfalls erleidet die Ladestation irreparable Schäden.



Chaos Computer Club

Chaos Computer Club hacks e-motor charging stations



Hacking-Wettbewerb: Pwn2Own-Teilnehmer knacken Tesla-Ladestation

Offensichtlich sind Infotainmentsysteme und Ladestationen nicht effektiv abgesichert: Fast jede Attacke auf dem Pwn2Own Automotive 2025 war erfolgreich.

The EV Charger Hack That Can Burn Down Your House Just Got More Terrifying

Trend Micro researchers found a hack to remotely disable overheating protection in most home EV chargers. The results, which we got to see at Black Hat, were explosive.

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Isle of Wight: Council's electric vehicle chargers hacked to show porn site

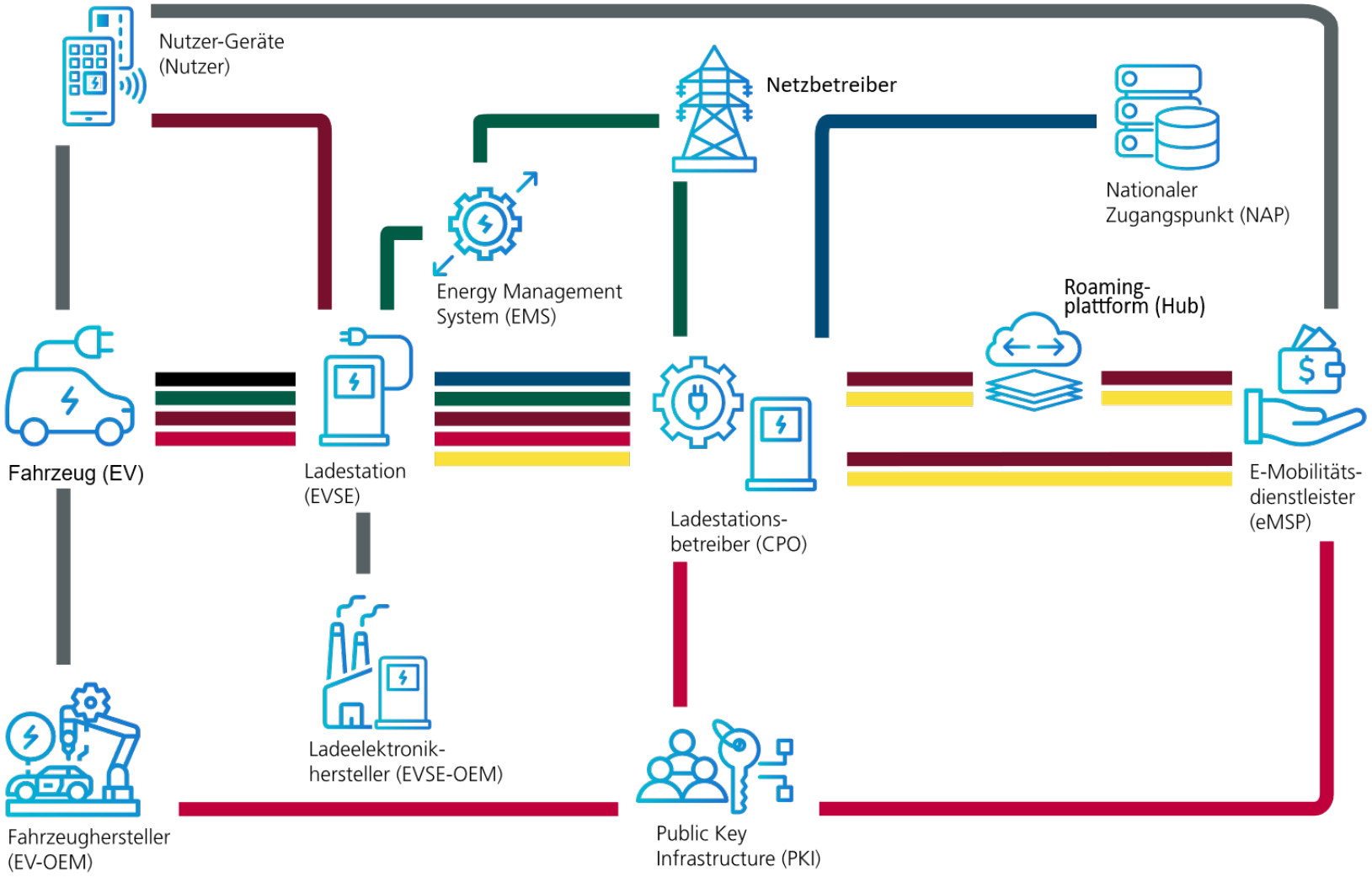
6 April 2022

Share Save

[2]

Systemlandschaft der öffentlichen Ladeinfrastruktur

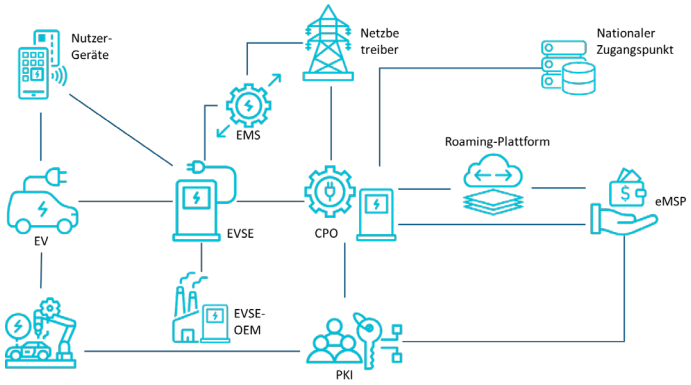
Vereinfachtes Modell



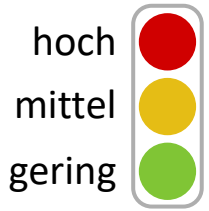
- Ladekommunikation
- Autorisierung
- Energieversorgung
- Abrechnung
- Systemverwaltung
- Zertifikatsverwaltung
- Proprietär

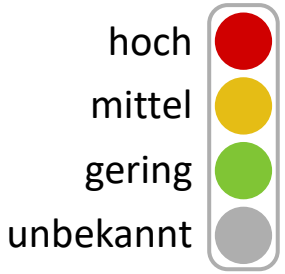
Dreizehn Gefährdungssteckbriefe wurden entwickelt

Aufbau der Gefährdungssteckbriefe



1. **Einteilung in Kommunikationsbeziehungen / Aspekte der öLIS**
   - Beschreibung (Protokolle, Schnittstellen, beteiligte Akteure, …)
   - Schwerpunkt: Ladekommunikation, Roaming, Zertifikatsverwaltung, …
2. **Einschätzung Schadenspotential**
   - Ausprägung: Verfügbarkeit, Netzstabilität, finanzielle Schäden
   - Reichweite: lokal, regional, national
   - Einordnung mittels Ampelsystem
3. **Einschätzung der Gefährdungslage**
   - Berücksichtigung des Schadenspotentials
   - Eintrittswahrscheinlichkeit
     - Optionale Anforderungen / Design-Schwächen
     - Bekannte Schwachstellen





Gefährdungssteckbriefe öffentliche Ladeinfrastruktur

In Summe zeigt Analyse zur Vernetzung mittlere bis hohe Gefährdungslage auf

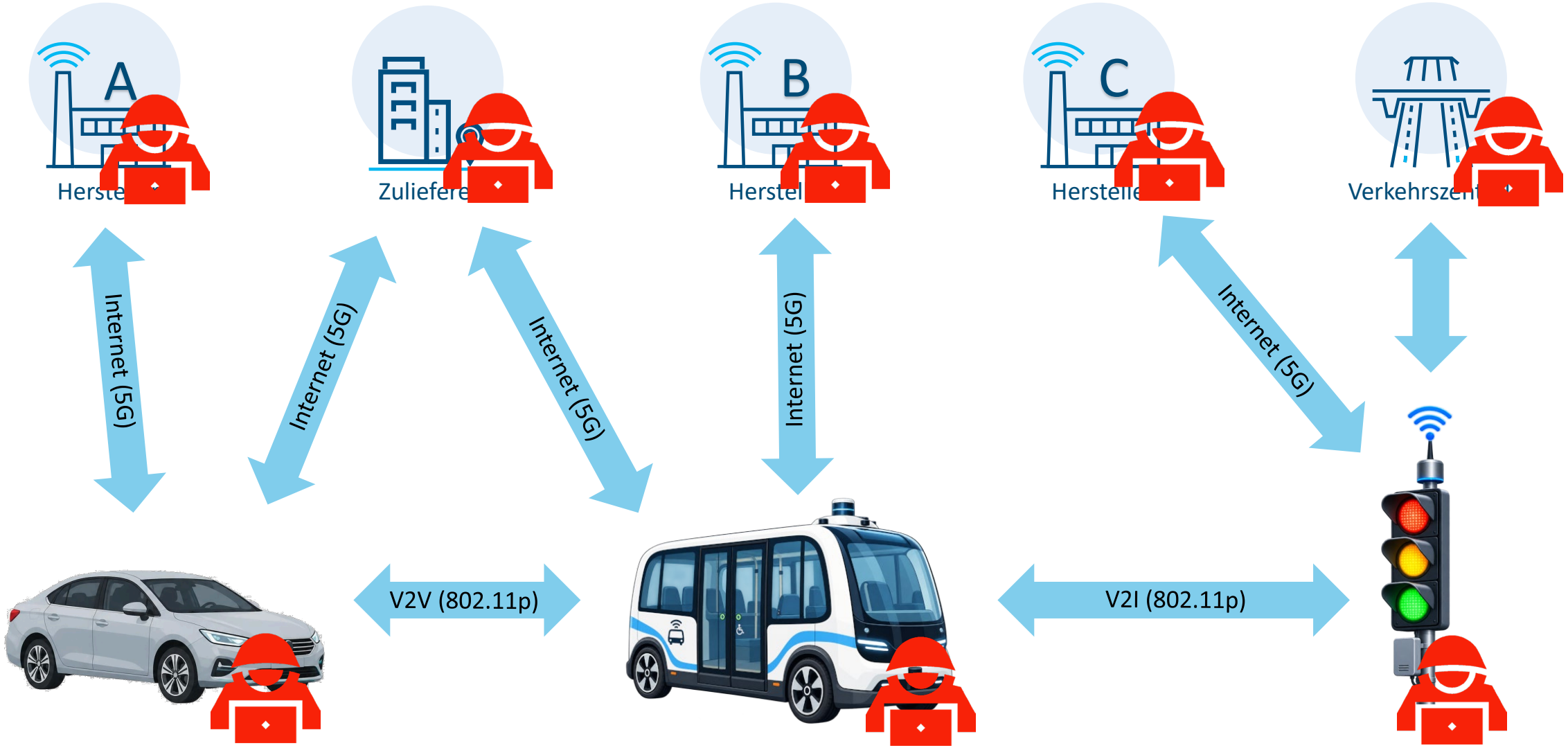
Nr.	Bezeichnung	Akteure / Verbindungen	S	G
1	Ladekommunikation	EV – EVSE		
2	Backendkommunikation – Fahrzeug	EV – EV-OEM		
3	Nutzerinteraktion mit dem Fahrzeug	EV – Nutzer		
4	Ladesäulenverwaltung und -steuerung – öffentlicher Bereich	EVSE – CPO		
5	Nutzerinteraktion mit der Ladestation	EVSE – Nutzer		
6	Backendkommunikation – Ladesäule	EVSE – EVSE-OEM		
7	Zertifikatsverwaltung und -Prüfung	PKI – EV-OEM, CPO, CSMS, eMSP		
8	Roamingkommunikation	CPO, eMSP, Hub		
9	Nutzerinteraktion mit Mobilitätsplattformen	eMSP – Nutzer		
10	Datenbereitstellung von öffentlich zugänglichen Datenpunkten	CPO – NAP		
11	Ladesäulenverwaltung und -steuerung – halböffentlicher Bereich	EVSE – EMS		
12	Interaktion mit dem Stromversorgungsnetz – halböffentlicher Bereich	EMS – Netzbetreiber		
13	Interaktion mit dem Stromversorgungsnetz – öffentlicher Bereich	CPO – Netzbetreiber		

Vorschläge für eine Verbesserung der Cybersicherheit der öffentlichen LIS

Nr.	Name der Maßnahme	Mehrwert	Aufwand	Priorisierung
1	Monitoringbericht zur Sicherheit in der öffentlichen Ladeinfrastruktur	+++	Höherer	Mittelfristig
2	Identifizierung von Problemfeldern für die Interoperabilität entlang der Wirkkette Laden	+	Niedriger	Zeitnah
3	Evaluierung der Anwendbarkeit intelligenter Messsysteme in der öffentlichen Ladeinfrastruktur	+	Niedriger	Zeitnah
4	Entwicklung einheitlicher technischer Mindeststandards	++	Erheblicher	Mittelfristig
5	Entwicklung von Anforderungen für interoperable PKIs innerhalb der öffentlichen Ladeinfrastruktur	++	Erheblicher	Mittelfristig
6	Technische Maßnahmen zur Kryptoagilität in der öffentlichen Ladeinfrastruktur	++	Höherer	Mittelfristig
7	Leitfaden für die sichere Inbetriebnahme von Systemen der öffentlichen Ladeinfrastruktur	++	Höherer	Zeitnah bis Mittelfristig
8	Verwendung von sicheren TLS-Versionen	++	Erheblicher	Mittelfristig
9	Härtung der Firmware von Ladestationen	+	Niedriger	Zeitnah
10	Anforderungen an sichere Kommunikation wesentlicher Bereiche der Ladeinfrastruktur im Rahmen der AFIR	+++	Höherer	Zeitnah
11	Konsequente Anwendung des CRA in der öffentlichen Ladeinfrastruktur	+++	Niedriger	Zeitnah

Cybersicherheit vernetzter Fahrzeuge

Vernetzung im Straßenverkehr

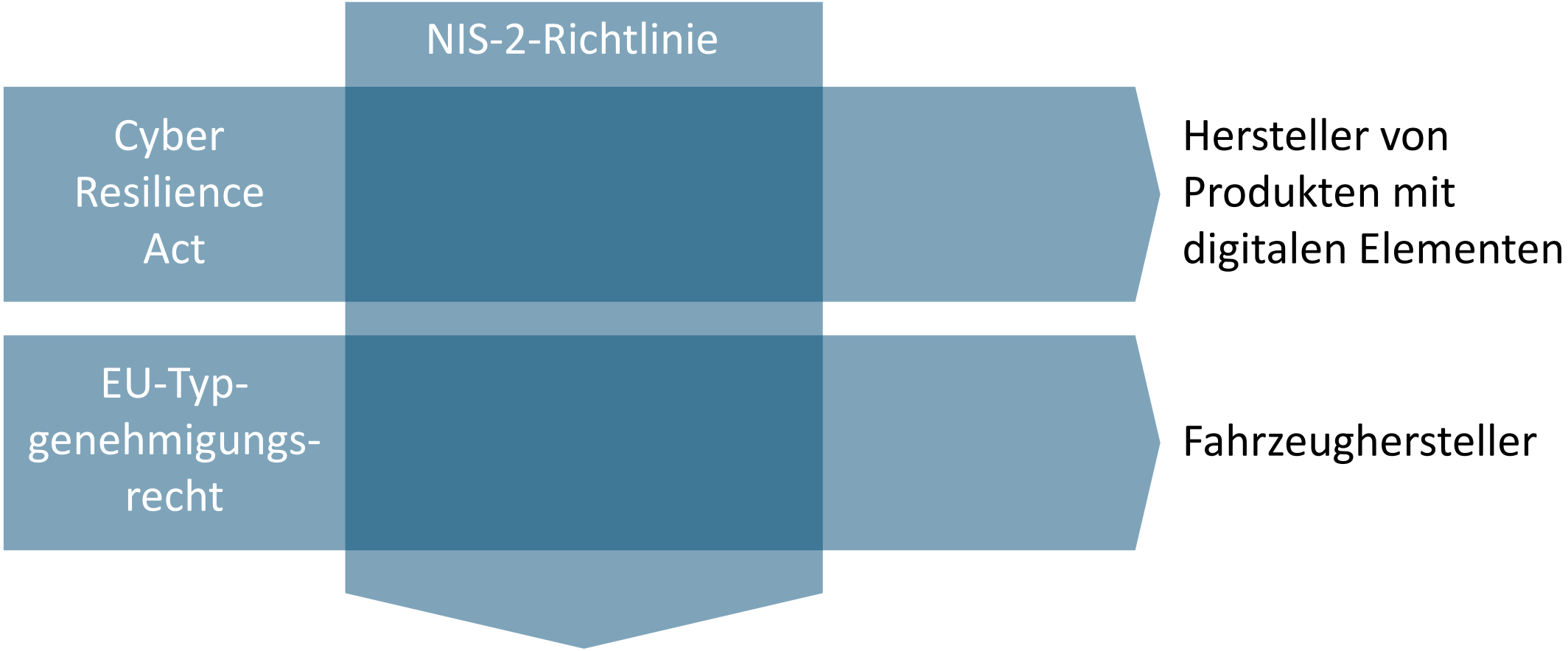


Regulierung

Bild: © AdobeStock/Azazul

Regulierung der Cybersicherheit im Gesamtsystem

CRA, Typgenehmigungsregulierung und NIS2-Richtlinie setzen unterschiedliche Hebel an



Ausgewählte Anforderungen des CRA

Produktanforderungen

- Angemessenes Cybersicherheitsniveau auf Basis einer Risikobewertung
- Cybersicherheit im Design-, Entwicklungs- und Produktionsprozess (Security-by-Design)
- Sichere Grundkonfigurationen (Security-by-Default)
- Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit

Anforderungen zum Umgang mit Schwachstellen

- Entgegennahme von Schwachstellenmeldungen und Durchführung regelmäßiger Sicherheitstests
- Angemessene Behandlung von Schwachstellen
- Bereitstellung von kostenlosen Sicherheitsupdates + Hinweismeldungen an Benutzende
- Öffentliche Information über Schwachstellen- und Schwachstellenbehebung

(Dritt-)Komponenten und sichere Lieferkette

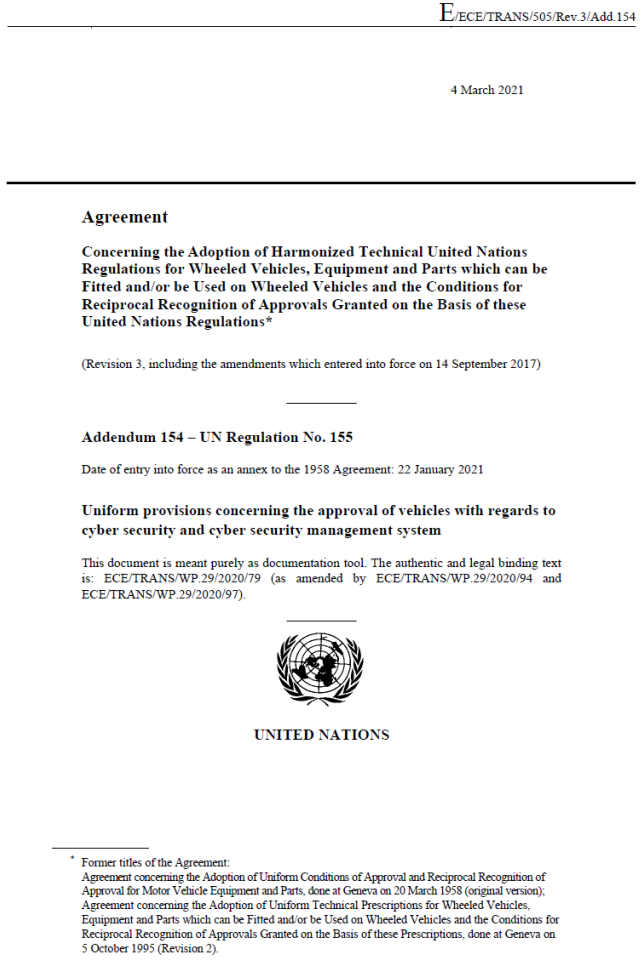
- Softwarestückliste (SBOM) erfasst (Dritt-)Komponenten
- Sorgfaltspflicht bei der Verwendung von (Dritt-)Komponenten
- Nachverfolgung und Weiterleitung möglicher Schwachstellen an Lieferanten

Mindestinformationen von Herstellern an Anwendende

- Benennung einer Kontaktstelle für Informationen über Schwachstellen
- Information zur Produktidentifizierung (Typ, Version, …)
- Angaben über die bestimmungsgemäße Verwendung
- Zugriffsmöglichkeiten auf die EU-Konformitätserklärung und ggf. verfügbare SBOM

UNECE-Regelung Nr. 155

- „Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system“
- In Typgenehmigungs-Verordnung (EU) 2019/2144 referenziert
- Umsetzung eines CSMS durch den Fahrzeughersteller
  - Prozesse, Verantwortlichkeiten und Governance für die Risikobehandlung im Hinblick auf Cyber-Bedrohungen and Angriffe
  - Soll Entwicklung, Produktion und Post-Produktion umfassen
- Risikobewertung muss Bedrohungen zu folgenden Kategorien umfassen
  - Back-End-Server mit Bezug zu Fahrzeugen auf der Straße
  - **Kommunikationskanäle**
  - Update-Verfahren
  - Unbeabsichtige Handlungen, die einen Cyberangriff begünstigen
  - **Externe Vernetzung und Verbindungen**
  - Fahrzeugdaten, -code
  - Schwachstellen durch nicht ausreichenden Schutz oder Härtung



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

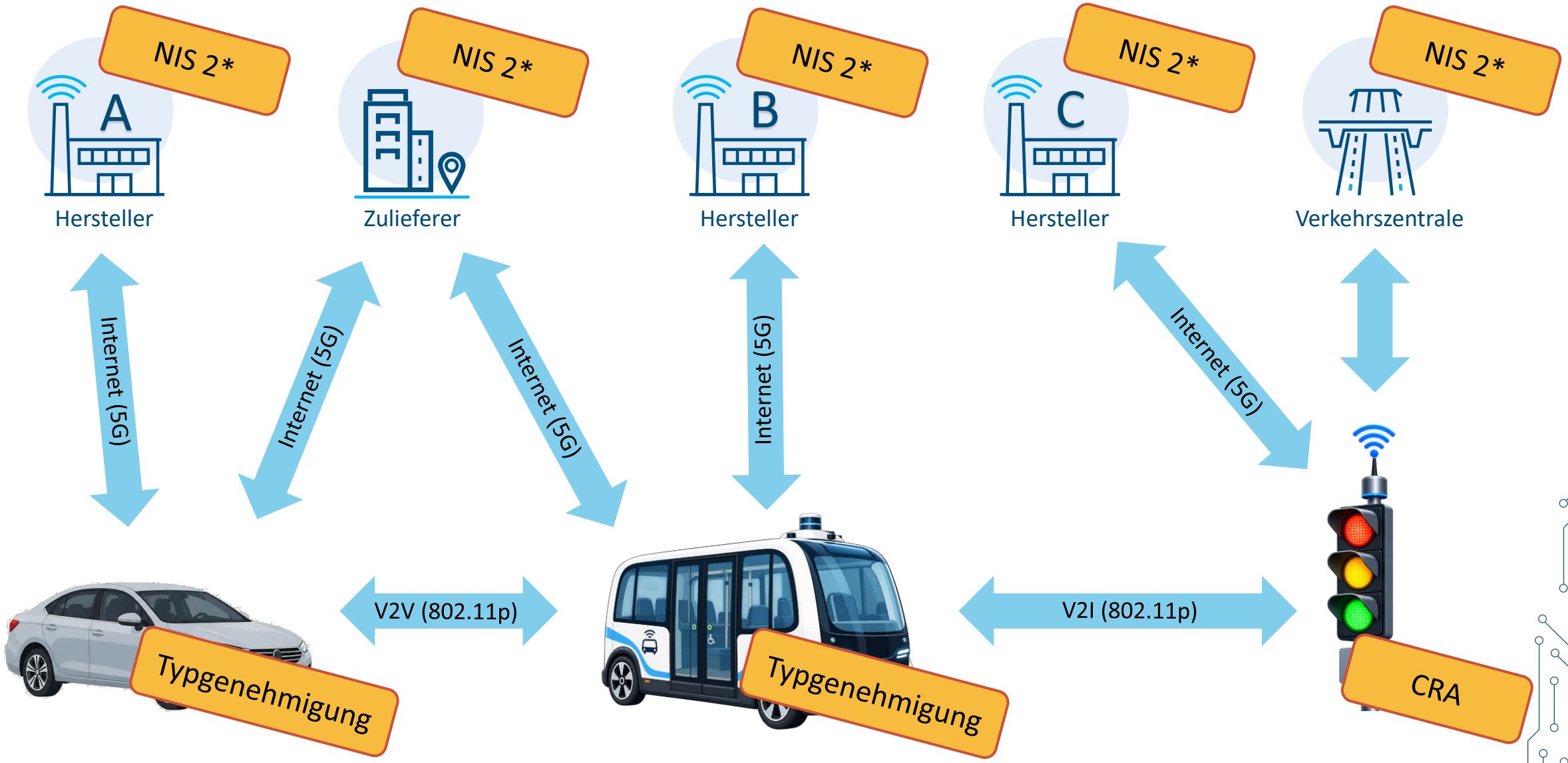
UNITED NATIONS

* Former titles of the Agreement:
Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

NIS-2-Regulierung im neuen BSI-Gesetz

- Maßnahmen zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU
- Einheitliches Sicherheitsniveau in den Mitgliedstaaten der EU schaffen und verbessern
- 06.12.2025: Umsetzung der NIS-2-RL in nationales Recht im BSI-Gesetz
- BSI wird für ca. 29.500 neue "besonders wichtige" (bwE) und "wichtige" Einrichtungen (wE) zur Aufsichtsbehörde; die bereits regulierten KRITIS werden eine Teilmenge der bwE
- Einführung von Registrierungs-, Meldepflichten für bwE und wE
- Unternehmen müssen angemessene, wirksame und geeignete Risikomanagement-maßnahmen umsetzen und dokumentieren
- Geschäftsführung trägt Verantwortung für Umsetzung, muss sich schulen lassen

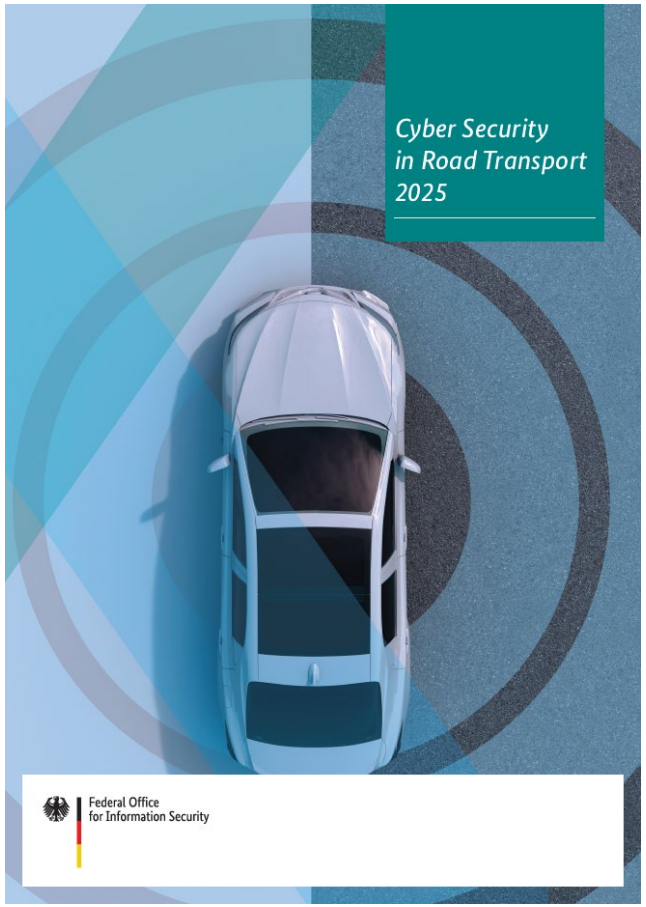
Vernetzung im Straßenverkehr



*Betroffenheit/Schwellwerte beachten

Weitere Informationen

BSI-Publikationen



https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/Cybersicherheit_Strassenverkehr_2025.html

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260728_Sichere_Ladeinfrastruktur.html

Fragen

Finden Sie Antworten:

- **Informationen zum Cyber Resilience Act**
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

- **NIS-2-Betroffenheitsprüfung**
  www.bsi.bund.de/dok/nis-2-betroffenheitspruefung

- **NIS-2-FAQ**
  www.bsi.bund.de/dok/nis-2-faq

Stellen Sie uns Fragen:
service-center@bsi.bund.de

Vielen Dank für Ihre Aufmerksamkeit!

Christian Wieschebrink

Referat D 23 – Verkehr und Industrie 4.0

automotive@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Backup

NIS 2: Mindestmaßnahmen Risikomanagement

Angemessen, wirksam und verhältnismäßig umsetzen, dokumentieren und ggf. überprüfen lassen, mindestens (!):

Konzepte Risikoanalyse und Sicherheit für Informationssysteme	**Bewältigung von Sicherheitsvorfällen**	**BCM und Krisenmanagement**	**Sichere Lieferkette**	**NIS-Sicherheits-maßnahmen und Schwachstellen-management**
Wirksamkeit von Risikomanagementmaßnahmen	**Schulungen und Sensibilisierung**	**Kryptografie/ Verschlüsselung**	**Sicherheit des Personals/ Zugriffskontrolle**	**MFA/ Authentifizierung, und sichere Kommunikation**

Ziel des Risikomanagements:
Störungen der **Verfügbarkeit, Integrität und Vertraulichkeit** der informationstechnischen **Systeme, Komponenten und Prozesse**, die sie für die **Erbringung ihrer Dienste** nutzen, zu **vermeiden** und **Auswirkungen** von Sicherheitsvorfällen möglichst gering zu halten.

Unterstützung für Unternehmen – Wie hilft das BSI?

Betroffenheitsprüfung

- Überprüfung, ob das Unternehmen von **NIS-2 betroffen** ist
- Basierend auf **Eigenauskünften**
- Ergebnis **rechtlich nicht verbindlich**

NIS-2-FAQ

- Sammlung von **Antworten** auf die am häufigsten gestellten **Fragen zur NIS-2-Richtlinie**
- Stand der **Gesetzgebung**
- Erste Details zu **gesetzlichen Pflichten**
- **Sektorspezifische Informationen**

NIS-2-Was tun?

- Was können Unternehmen jetzt schon tun, um sich auf NIS-2 **vorzubereiten**
- **Praktische Hinweise, Hilfestellungen**
- Wird stetig **ergänzt und aktualisiert**