TÜVNORD

Gebäudetechnik Webinar 2026

Wir geben Ihnen einen Wissensvorsprung

Navigieren durch NIS 2 und mehr

Referent: Klaus Kleine Büning TÜV NORD Infrachem

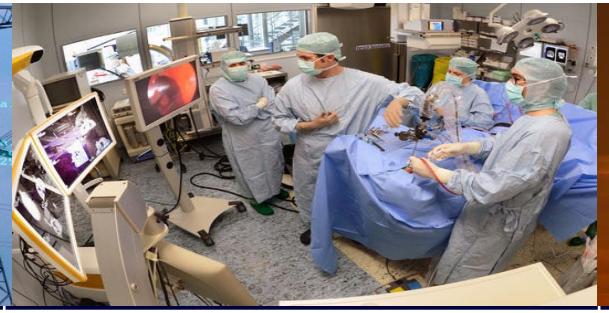
TÜVNORD

Normale Einstellung zu Cybersicherheit

Cyberangriffe auf die Industrie

2016: Computervirus im Kernkraftwerk

2016: Stromausfall in der Ukraine durch Cyberangriff



2015: Hacker kontrollieren Narkosegerät im Operationssaal

2015: Hacker übernehmen Passagiermaschine

2015: Hacker blockiert Gaspedal bei Jeep

2014: Hacker greifen Firma Bayer an

2014: Sasser: Wurm beeinträchtigt Zugkommunikation

2014: Hacker bringt Stahlwerk unter Kontrolle

Quelle: Deutscher Presse Dienst

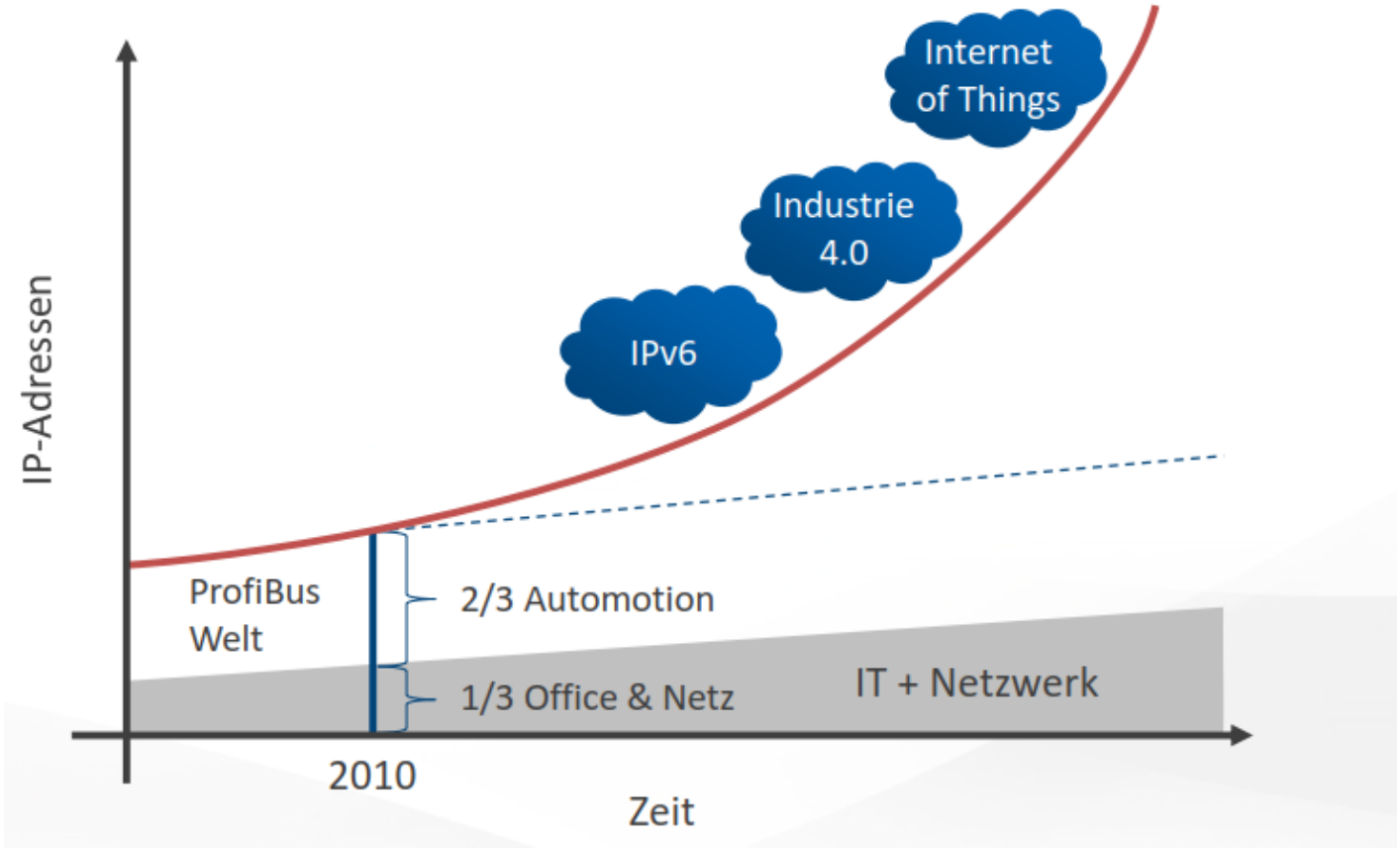
Es gibt heute eine echte Bedrohung durch Hacker und Schadsoftware für die Gesellschaft!

Wovon reden wir hier?

Ist Cybersicherheit nicht IT?

TÜVNORD

Wachsende Herausforderungen

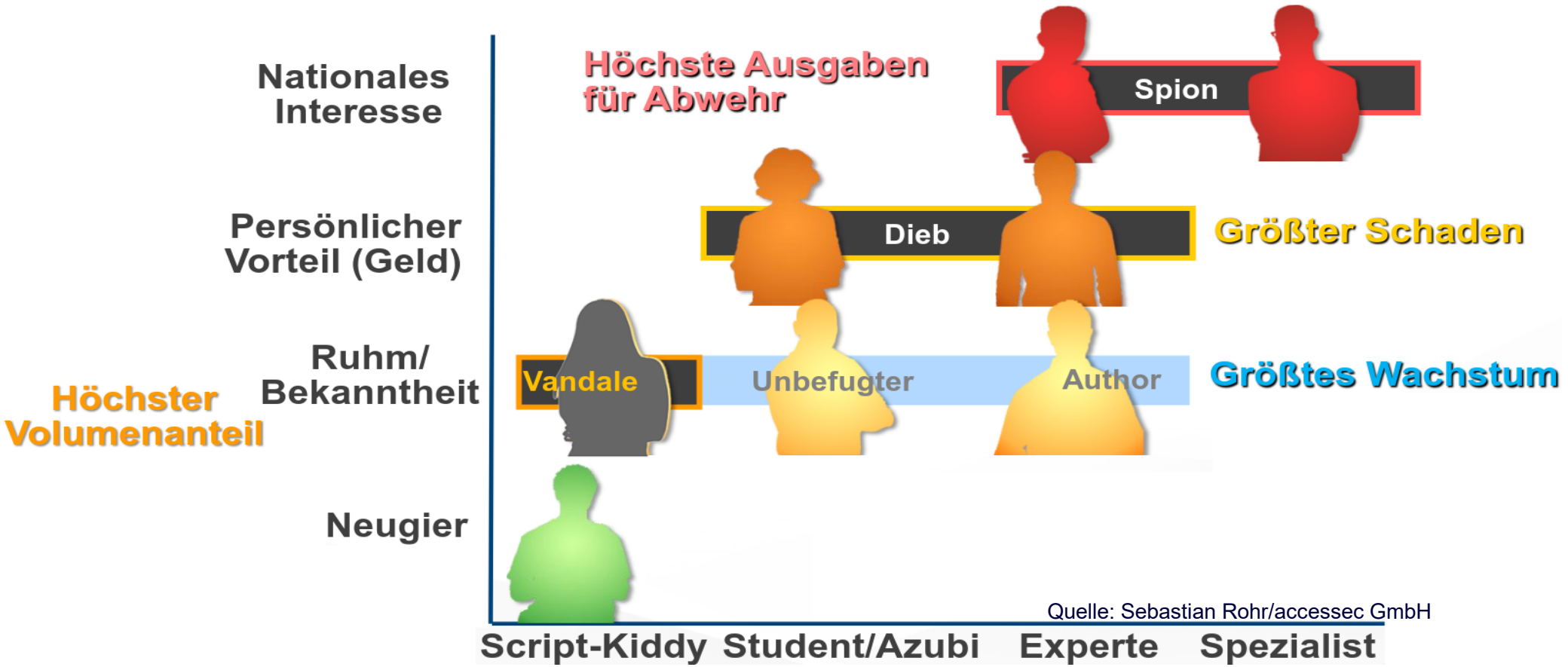


TÜVNORD

The Network and Information Security (NIS) Directive

2016	Inkrafttreten erster EU Cybersecurity-Richtlinie (NIS-1)
11/2017	Veröffentlichung des Leitfaden KAS-44 *Schutz vor cyberphysischen Angriffen*
09/2019	Veröffentlichung der Empfehlung 1115 *Umgang mit Risiken durch Angriffe auf die Cysi von sMSR-Einrichtungen*
11/2019	Veröffentlichung des Leitfaden KAS-51 *Maßnahmen gegen Eingriffe Unbefugter*
11/2022	Veröffentlichung der TRBS 1115-1 *Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen*
01/2023	EK ZÜS B-002 Stufe 1 *Hinweis auf Erfordernis*
04/2024	EK ZÜS B-002 Stufe 2 *Ordnungsprüfung auf Plausibilität*
2023	Inkrafttreten der zweiten EU Cybersecurity-Richtlinie (NIS-2)
12/2025	Umsetzung NIS-2 in deutsches Recht, EK ZÜS B002 Stufe 3, TRBS 1115-1 VCI-/VdTÜV-Leitfaden Cybersicherheit in der Prozessindustrie – Umsetzung und Prüfung

Bedrohungsszenarien



Quelle: Sebastian Rohr/accessec GmbH

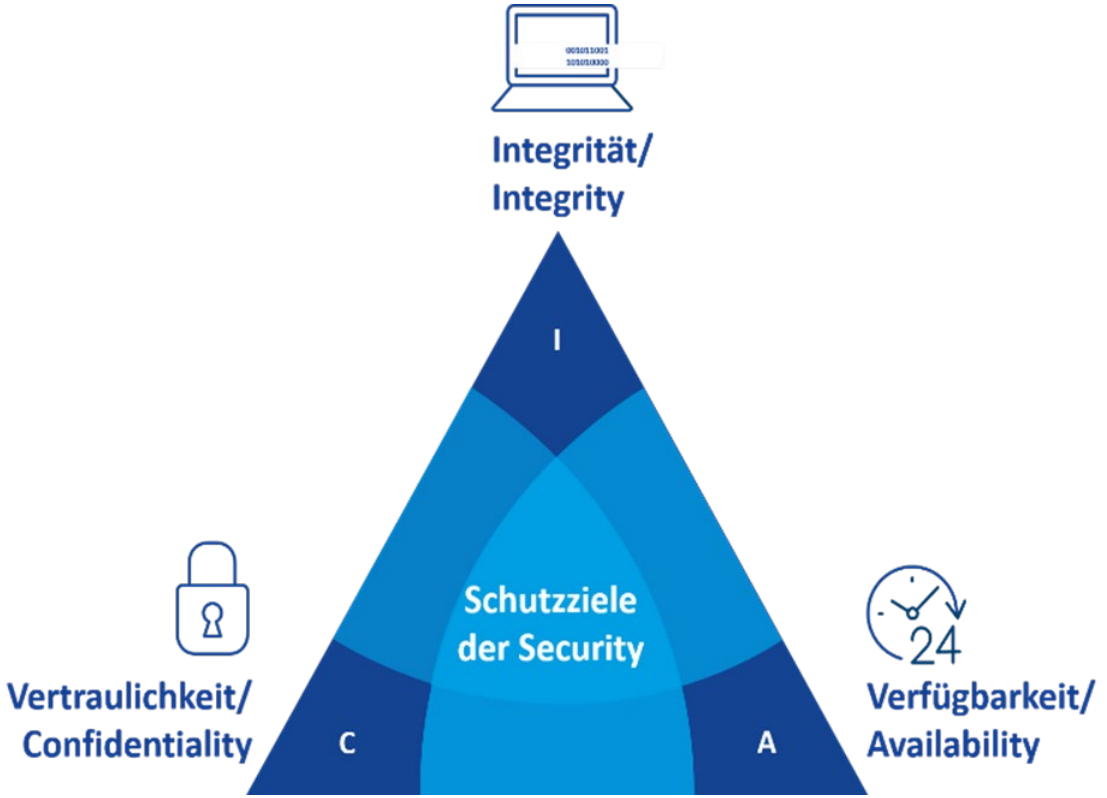
Mensch und Technik

- Verständnis des Menschen für die eingesetzte Technik
- Unterschiede zwischen IT und OT Schutzebenen
- Wachsende Automatisierung erfordert ein wachsendes Verständnis bei den Mitarbeitern

Beispiel Remoteverbindung

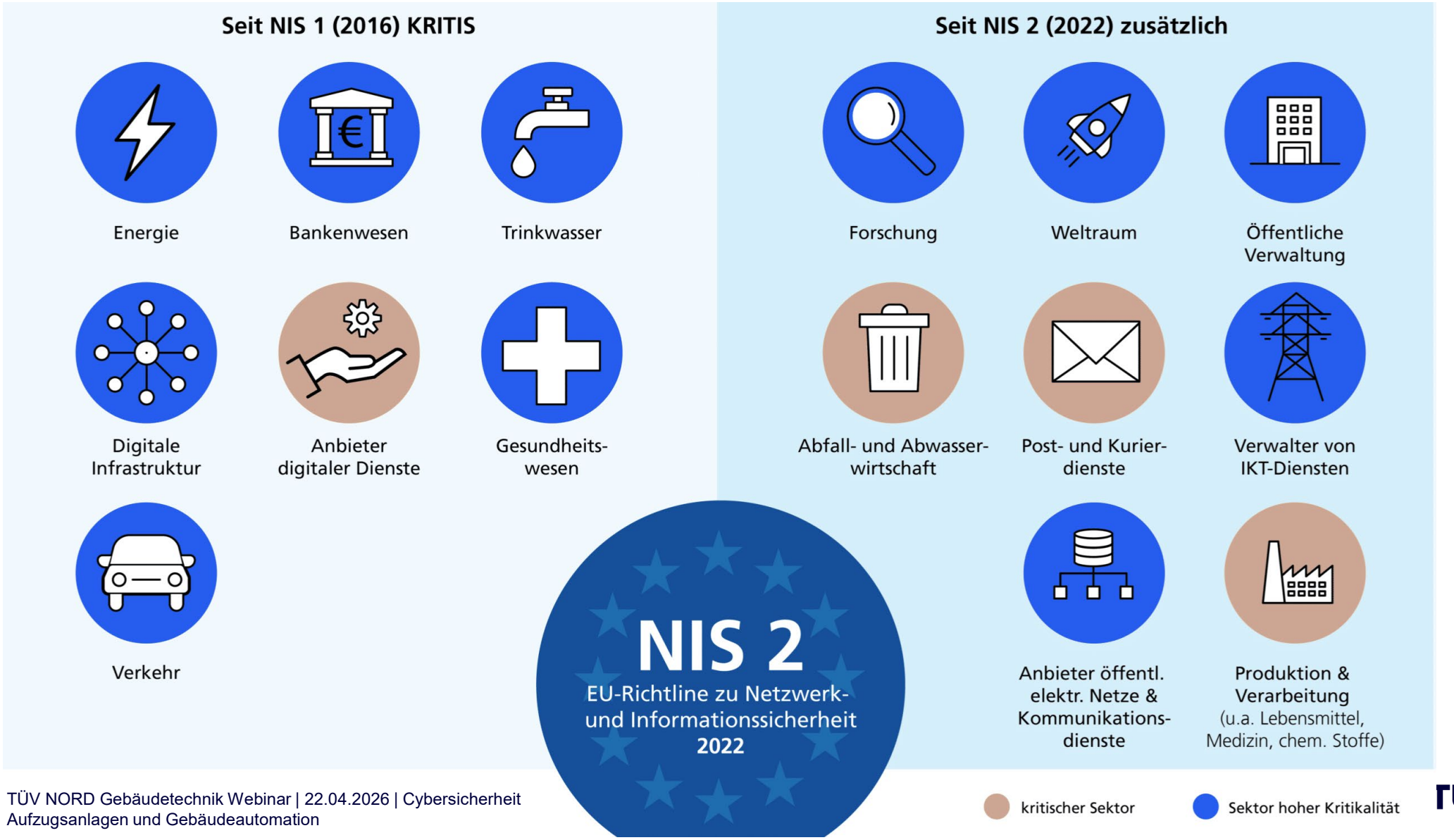
- Aus Sicht der Mitarbeiter wichtig
- Aus Sicht der Security gefährlich

(Schutzebenen)



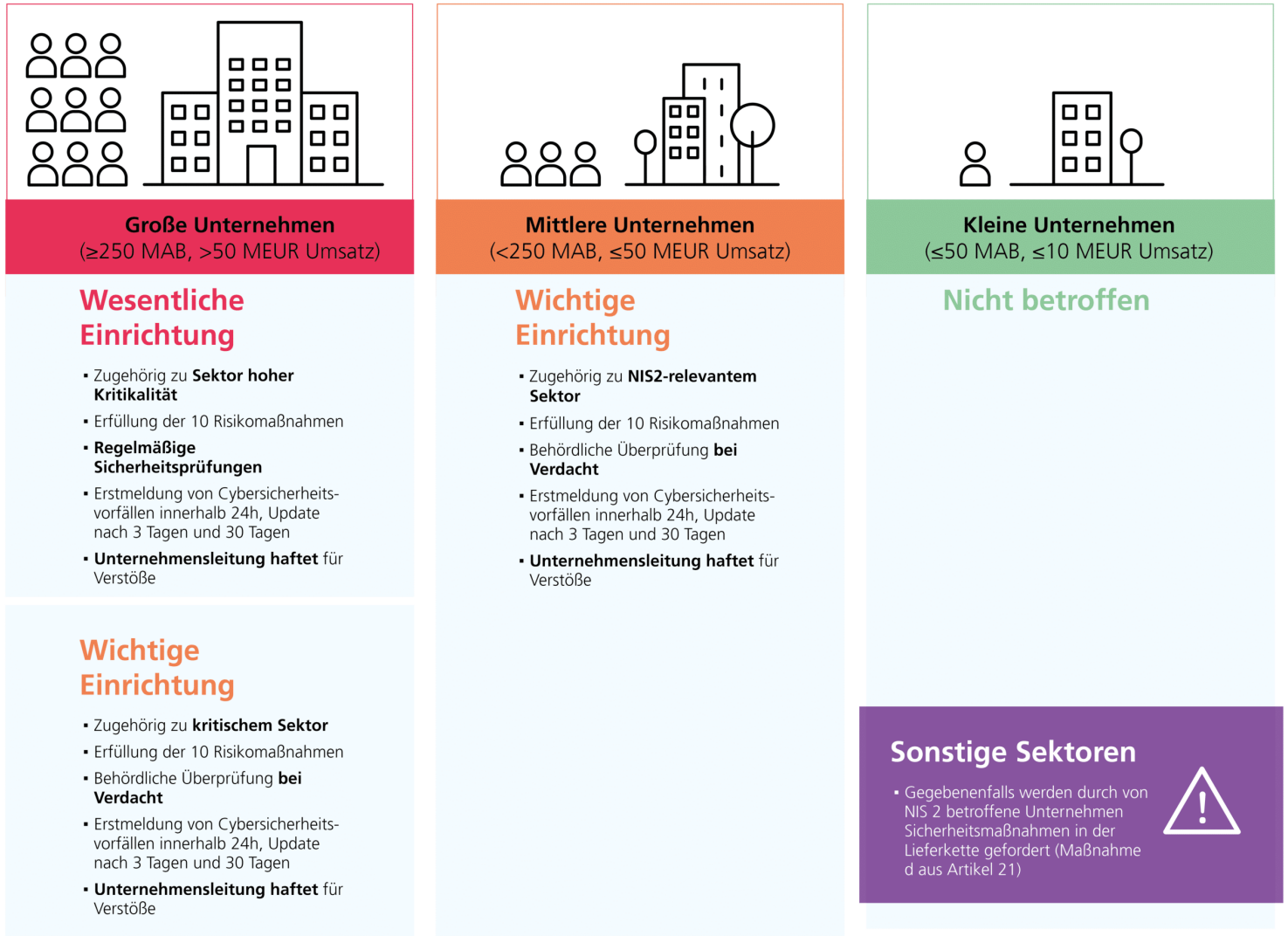
TÜVNORD

Welche Branchen betrifft die NIS2 Richtlinie?



Quelle: [NIS 2-Richtlinie: Zusammenfassung und Umsetzung für Deutschland - Blog des Fraunhofer IESE]

Welche Unternehmen betrifft die NIS2 Richtlinie?



Quelle: [NIS 2-Richtlinie: Zusammenfassung und Umsetzung für Deutschland - Blog des Fraunhofer IESE]

Maßnahmen aus NIS 2 Artikel 21

Für Risikomanagement und Resilienz

Vorbereitung auf Cybersicherheitsvorfälle

- **Risikoanalyse** und Sicherheit von Informationssystemen
- **Bewältigung** von Sicherheitsvorfällen
- **Aufrechterhaltung** des Betriebs

Geschäftsbeziehungen

- Sicherheit der **Lieferkette** (unmittelbare Anbieter und Dienstanbieter)
- Sicherheitsmaßnahmen bei **Erwerb und Wartung** von Netz- und Informationssystemen, einschließlich Management und Offenlegung von **Schwachstellen**

Kontrolle und Awareness

- Konzepte und Verfahren zur **Bewertung der Wirksamkeit** der Risikomanagementmaßnahmen
- Grundlegende Verfahren im Bereich **Cyberhygiene, Schulungen** im Bereich der Cybersicherheit

Technische Umsetzung

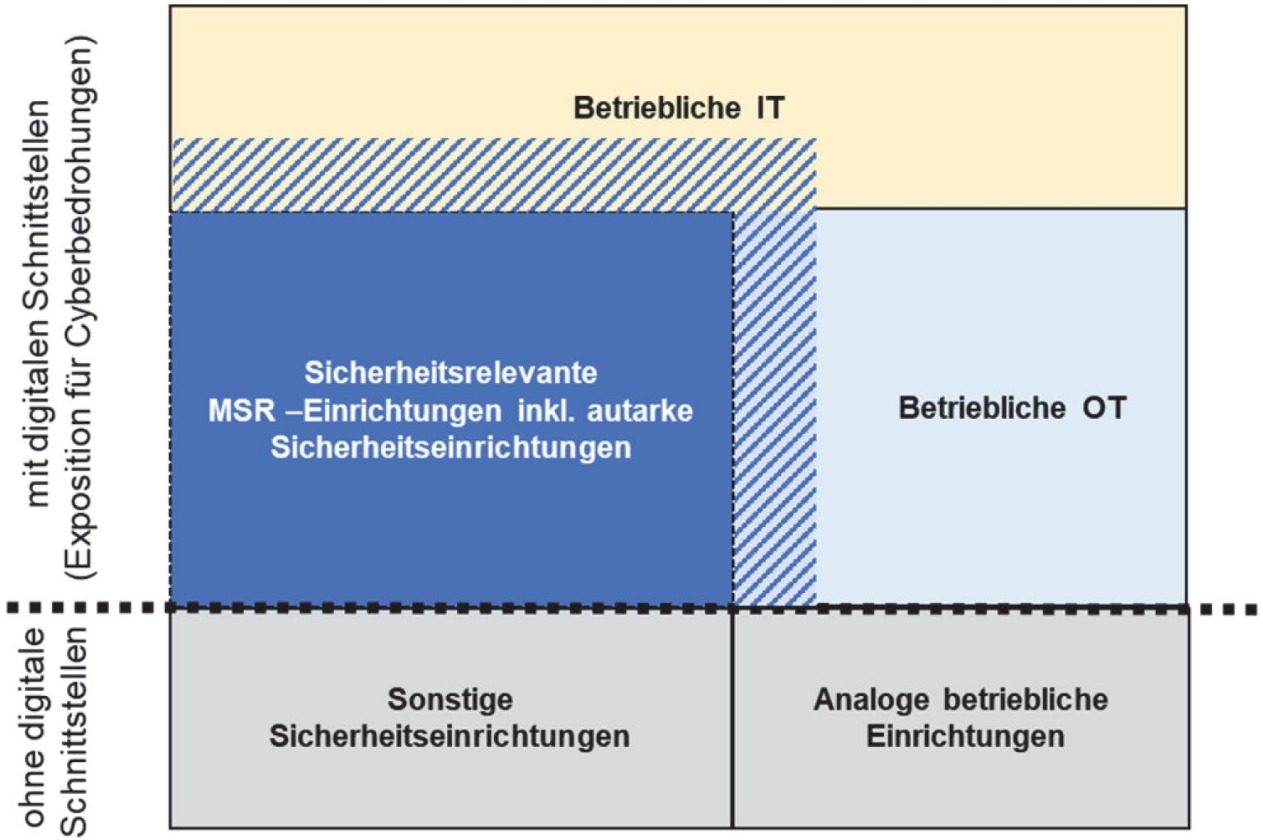
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und Verschlüsselung
- Sicherheit des Personals, Konzepte für **Zugriffskontrolle** und Management von Anlagen
- Verwendung von **Multi-Faktoren-Authentifizierung** oder kontinuierlicher Authentifizierung, **gesicherte Kommunikation** und ggfs. gesicherte interne Notfallkommunikation

Quelle: [NIS 2-Richtlinie: Zusammenfassung und Umsetzung für Deutschland - Blog des Fraunhofer IESE]

Prüfung nach BetrSichV

EK-ZÜS B-002 rev. 5

- **Prüfumfang wird um die „Funktionsprüfung“ erweitert**
- **Ordnungsprüfung wurde detailliert**
  - 14 Prüfschritte
- **Inhalte an die TRBS 1115-1 angepasst**
- **Neue TRBS 1115-1**
  - Anhang 2
  - Erläuterungen und Beispiele für erforderliche Cybersicherheitsmaßnahmen



TÜVNORD

Cyber Resilience Act (CRA): Scope und Ziel

gerichtet an Produkte

Scope

- Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen
- neuer, einheitlicher Rechtsrahmen für die Einhaltung der Cybersicherheitsvorschriften in der EU
- Verpflichtungen für Hersteller, Vertreiber und Importeure
- grundlegende Anforderungen an die Cyber-sicherheit während des gesamten Lebenszyklus
- Business Produkte wie auch Consumer Produkte
- Konformitätsbewertung - differenziert nach Risikograd
- Marktüberwachung und Durchsetzung

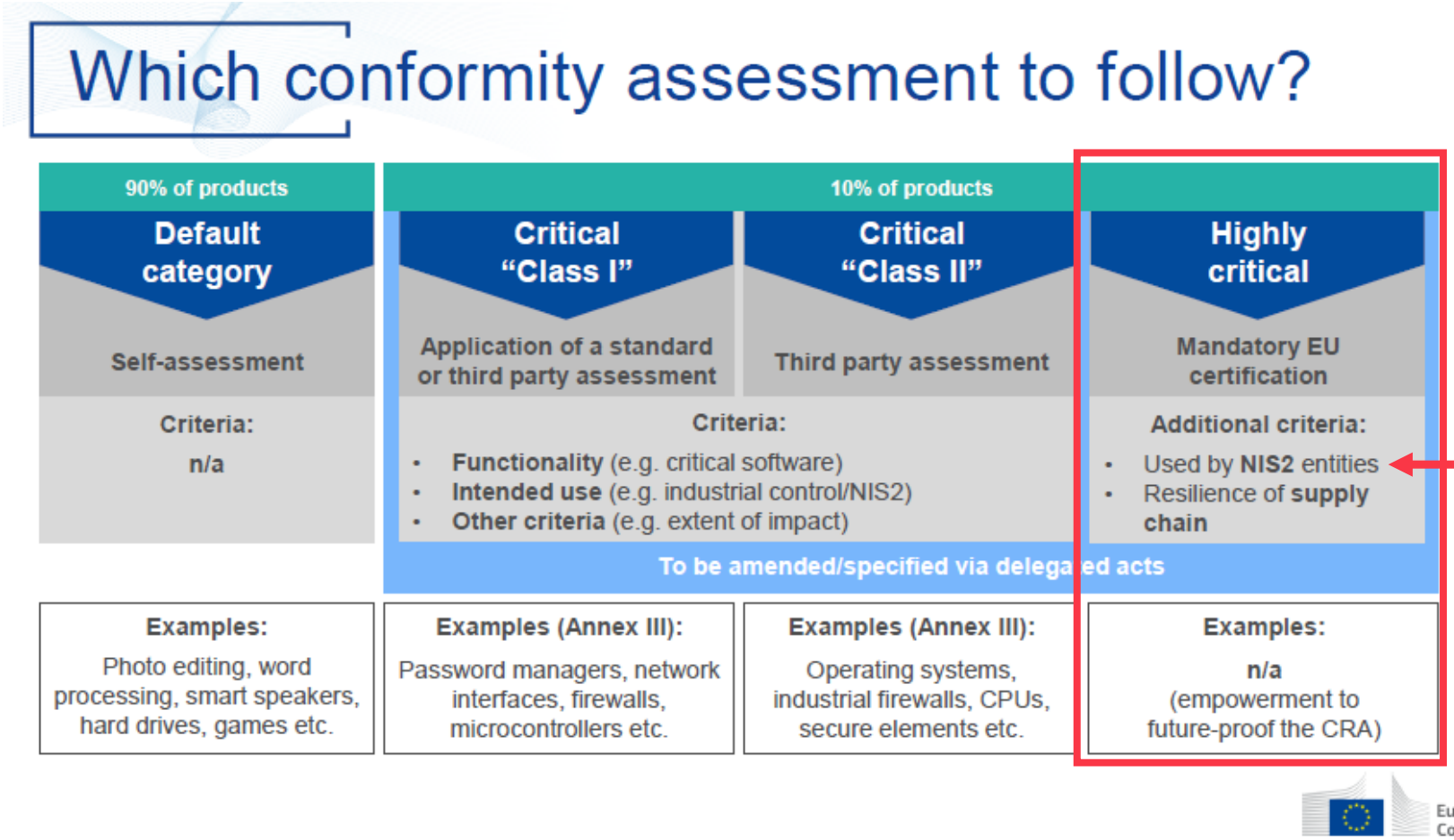
Ziele

- herstellerseitige Verantwortung für Sicherheit digitaler Produkte in Entwurfs- und Entwicklungs-phase und Verbesserung während des gesamten Lebenszyklus
- Gewährleistung eines kohärenten Rahmens für die Cybersicherheit, der die Einhaltung der Vorschriften für Hardware- und Softwarehersteller erleichtert
- erhöhte Transparenz der Sicherheits-eigenschaften und -praktiken von Produkten mit digitalen Elementen
- sichere Nutzung und Einsatz von digitalen Produkten für Unternehmen und Verbraucher zu ermöglichen

TÜVNORD

CRA: Konformitätsbewertung und Risikoklassen

Überblick

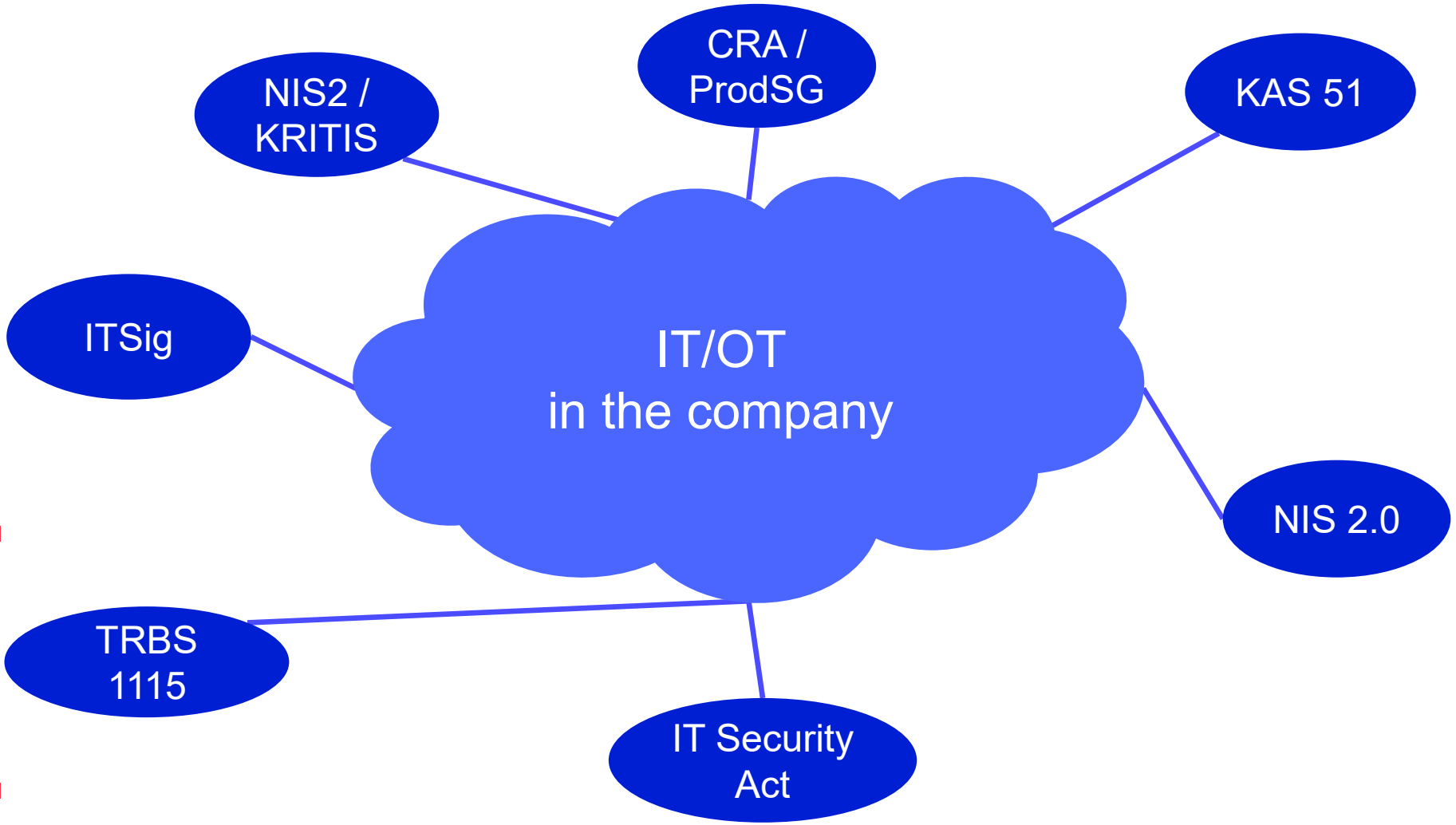


Wird noch festgelegt

- sog. delegierte Rechtsakte
- Wird für Produkte gelten, die kritisch für Resilienz der Lieferkette sind, oder von wesentlichen Einrichtungen genutzt werden.
- Produktzertifizierung nach EU CSA, beispielsweise **EUCC**

TÜVNORD

Legal Requirements



Cybersicherheit an Aufzugsanlagen

Referent: Peter Lübbe

Agenda

TÜV NORD Gebäudetechnik Webinar: Cybersicherheit an Aufzugsanlagen

- Vorstellung Referent Peter Lübbe
- Gesetzliche Grundlage
- Die TRBS 1115-1
- Gefahren für den Aufzug und seine Nutzer
- Beispiele möglicher Cyberangriffe
- TÜV Mangel Cybersicherheit
- Cybersicherheit → ein Bestandteil der Gefahrenanalyse / Gefährdungsbeurteilung

Vorstellung Peter Lübbe

TÜV NORD Gebäudetechnik Webinar: Cybersicherheit an Aufzugsanlagen

- Zur Person
  - seit 2012 beim TÜV Nord in Mecklenburg-Vorpommern
  - Sachverständiger für Aufzüge, Hebezeuge, Elektrotechnik
  - Profit-Center Leiter mit 22 Sachverständigen

- Wir prüfen in den folgenden Fachgebieten:
  - Fördertechnik: Aufzüge, Hebezeuge, Krane, fliegende Bauten, Bühnentechnik
  - Elektrotechnik: VdS, PV-Anlagen, DGUV
  - Baurecht: Brandmeldeanlagen, Sicherheitsstromversorgungen, Lüftungsanlagen
  - Spielplätze und Spielgeräte

Gesetzliche Grundlagen

Cybersicherheit an Aufzugsanlagen

- Hersteller sind nach dem Produktsicherheitsgesetz (ProdSG) angehalten eine Risikoanalyse zu erstellen und diese auf dem aktuellen Stand der Erkenntnisse zu halten. Cyberangriffe über Remotezugänge sind bereits aufgetreten und sollten daher ebenfalls durch die Risikoanalyse berücksichtigt werden Durch den steigenden Vernetzungsgrad können sicherheitsrelevante MSR-Einrichtungen zunehmend zum Ziel von Cyberbedrohungen werden.

- Betreiber von Aufzugsanlagen sind nach BetrSichV (siehe TRBS 1115-1) aufgefordert auf der Grundlage von Cyberrisikoanalysen wirksame Security Maßnahmen zu treffen.
  - Die TRBS 1115-1 unterstützt den Betreiber bei der Vorgehensweise zur Ermittlung von Cybergefährdungen

Die TRBS 1115-1

Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

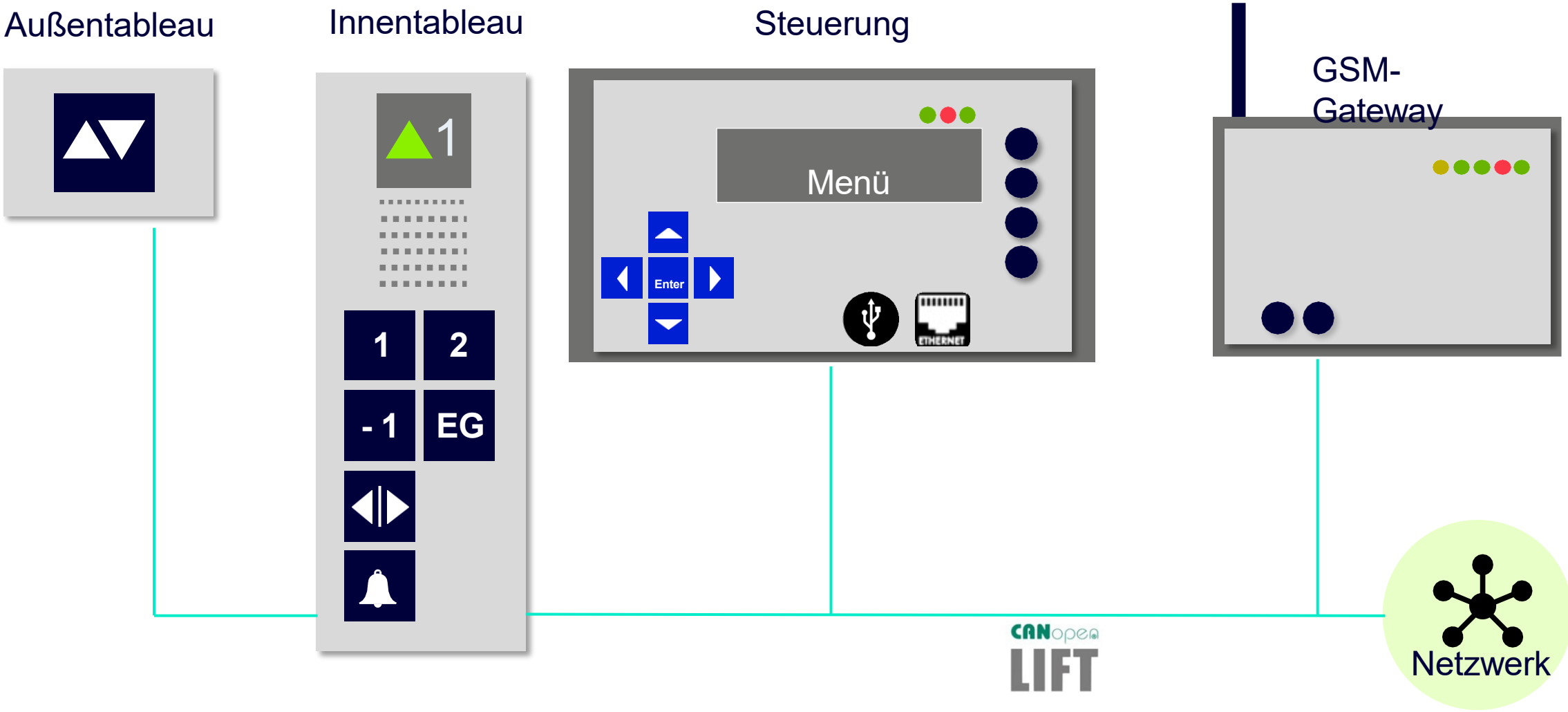
- Durch den steigenden Vernetzungsgrad können sicherheitsrelevante MSR-Einrichtungen zunehmend zum Ziel von Cyberbedrohungen werden.
- Der Arbeitgeber muss:
  - Gefährdungen beurteilen
  - Maßnahmen zur sicheren Verwendung ableiten
  - Gefahren für Beschäftigte und andere Personen vermeiden
  - Verfahren etablieren, um die Eignung und Funktionsfähigkeit der Cybersicherheitsmaßnahmen zu überprüfen → regelmäßige Neubewertung der Maßnahmen
  - Maßnahmen dokumentieren
- wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV → „Hauptprüfung“ an Aufzugsanlagen

Gefahren für den Aufzug und seine Nutzer

Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

- Zunehmende Menge an Meldungen von unautorisierten Zugriffen und Schadcode-Attacken
- Zunehmender Einsatz von Standardsoftware und -hardware in Kontroll- und Steuerungssystemen
- Die Implementierung des IP-Protokolls setzt Kontrollsysteme den gleichen Schwachstellen aus wie IT-Systeme
- Zunehmende Nutzung von Fernüberwachung und –steuerung von Anlagen

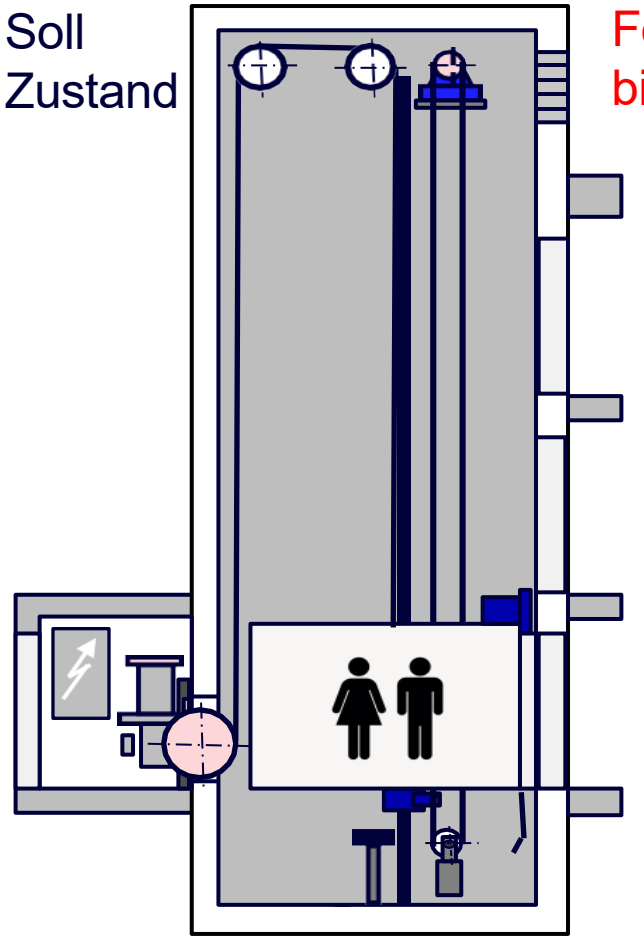
Fallbeispiel Aufzugssteuerung (1)



TÜVNORD

Fallbeispiel Aufzugssteuerung (2)

Soll Zustand



Fehler-bild

1. Passagier ruft über Außentableau den Aufzug in das Stockwerk YX
2. Aufzugsteuerung schließt die Tür nicht
3. Steuerung fährt Aufzug ins Stockwerk XY nicht
4. Aufzugsteuerung öffnet die Tür nicht
5. Passagier steigt in den Aufzug
6. Passagier wählt das Ziel-stockwerk YZ
7. Aufzugsteuerung schließt die Tür nicht
8. Aufzugsteuerung fährt Aufzug ins Stockwerk YZ nicht
9. Aufzugsteuerung öffnet die Tür nicht

Folgen

➡ Anlage unverfügbar

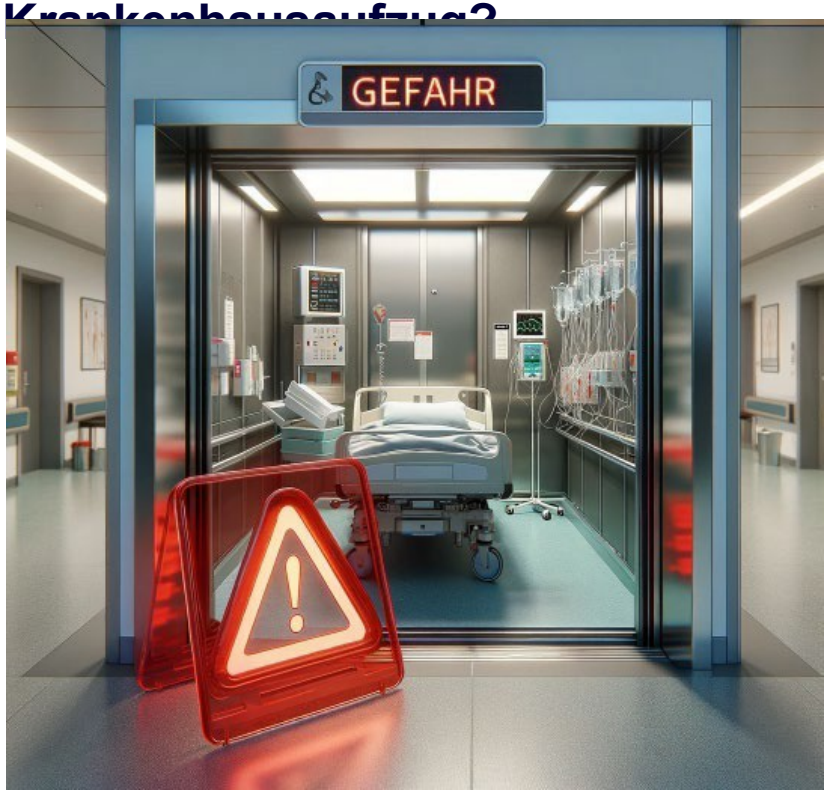
➡ erhöhte Unfallgefahr

➡ Personeneinschlüsse

TÜVNORD

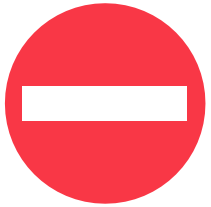
Fallbeispiel Aufzug (3)

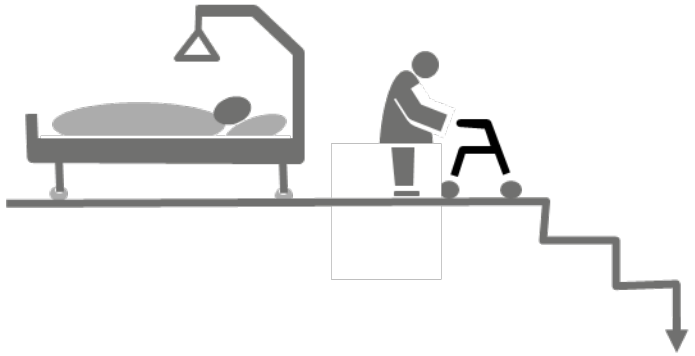
Was bedeutet dies z.B. für einen Krankenhausaufzug?



1. Transportmittel für bis zu 100 Mitarbeitern und unzähligen Gästen
2. Patiententransport mit Betten
3. Transport empfindlicher medizinischer Geräte
4. Notstromgesicherter Betrieb

Einschränkungen beim Ausfall





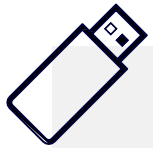
Aufgrund der besonderen Bedeutung von Krankenhausaufzügen sollten für deren Bau und Betrieb heute auch Cyberrisiken untersucht und durch Schutzmaßnahmen behandelt werden.

TÜVNORD

Welche Sicherheitsaspekte müssen u.a. beim Aufzug berücksichtigt werden?

Zugang

Ist der Zugang zu Komponenten der Aufzugssteuerung und zum Triebwerksraum nur autorisierten Personen möglich?



Physischen Schnittstellen

Gibt es physische Schnittstellen (z.B. Programmier-schnittstellen, USB) zur Aufzugssteuerung bzw. anderen Aufzugskomponenten?

Drahtlose Schnittstelle

Gibt es drahtlose Schnittstellen (z.B. Bluetooth, WLAN) an Aufzugs-komponenten?

Fernnotruf

Bestehen Schnittstellen zwischen der Fernnotrufanlage und der Aufzugsteuerung?

Bewertung der Cybersicherheit an Aufzugsanlagen

Der Mangel 843A: „Eine Dokumentation zur Cybersicherheit nach TRBS 1115-1 liegt nicht vor“

- Was ist zu tun?
  - Laden Sie sich das Formular zu Bewertung der Cybersicherheit von TÜV NORD herunter.
  - Füllen Sie das Dokument mit Ihrem Errichter oder Ihrer Wartungsfirma aus.
  - Hinterlegen Sie das Dokument an ihrer Aufzugsanlage!
  - Prüfen sie regelmäßig die Aktualität!

Bewertung der Cybersicherheit an Aufzugsanlagen

- Das Dokument beinhaltet eine Handlungsanweisung
- Ein Beispiel verdeutlicht mögliche Schnittstellen
- Tragen sie ihre spezifischen Anlagen Daten in die Tabelle ein
- Sollten Sie mehrere Aufzüge haben, ist für jeden Aufzug eine separate Bewertu zu erstellen.

Beispiele für Steuerungsbauarten, gefährdete Schnittstellen und mögliche Maßnahmen

Aufzugssteuerung Bauart		Schütz / Relais	Microcontroller-Steuerung	Weitere Komponenten (z.B. PESSRAL, FU)	Mögliche Maßnahmen (nach TRBS 1115-1)
Netzwerk-schnittstellen		Notruf-system	Notrufsystem Fernzugriff auf Steuerung	---	Firewall / Passwortschutz / …
Hardware- und Benutzer-schnitt-stellen	draht-gebunden	---	RS 232	USB	Schnittstelle unter Verschluss halten, im Schaltschrank oder Triebwerksraum, Zugangsbeschränkungen…
			USB	LAN	
			LAN, CANopen	CANopen	
	nicht draht-gebunden	---	W-LAN	---	Firewall / Passwortschutz / …
			Bluetooth	---	
			sonstige Funkschnittstelle	---	

Die 4 Mythen bezüglich der Cybersecurity von OT- Systemen

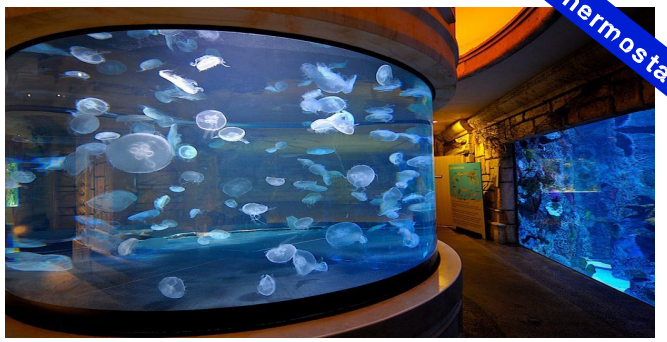
Mythos 1: Unsere Anlagen und Einrichtungen sind kein Zielobjekte!

2017: Hacker sperren Hotelgäste aus

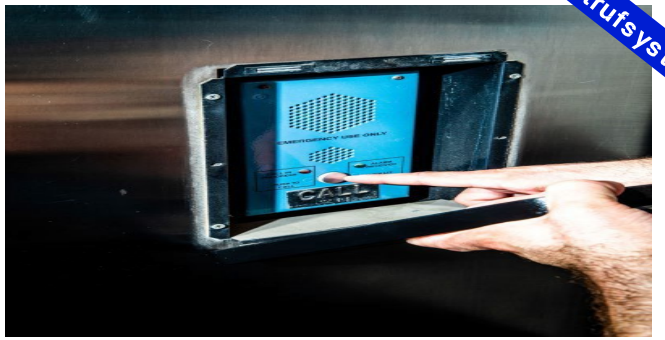
2014: Alarmierungsanlage mit 10 € Equipment ausgeschaltet

2017: Fremdgesteuerte Überwachungskameras

2016: Schadsoftware lähmt Krankenhaus in Neuss und Arnsberg



2018: Datendiebstahl eines Casinos durch hack des digitalen Thermostats im Lobby-Aquarium

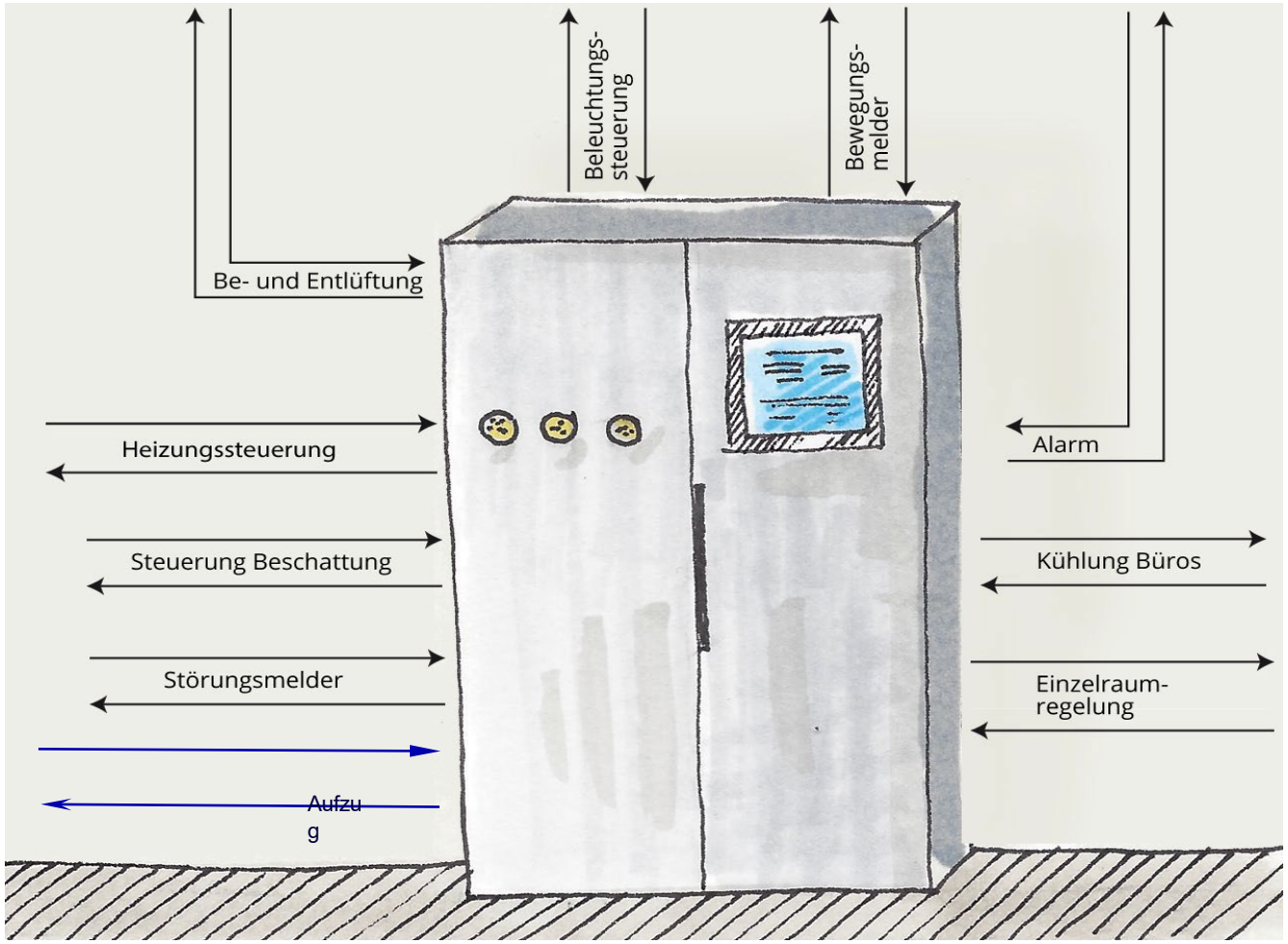


2019: Demonstration eines Aufzug-Hacks über das Notrufsystem

TÜVNORD

Mythos 2: Unsere Anlagen sind nicht mit dem Internet verbunden!

- Es benötigt keine Verbindung zum Internet, um angegriffen zu werden. Durch einen einfachen USB-Stick oder ein Wartungstool kann die Steuerung bereits kompromittiert werden.
- Bei den meisten GLT-Systemen besteht eine unbekannte Verbindung zum Office-IT-Netz (Provisorium)
- Verschiedene Komponenten können eigenständige Internetverbindungen aufbauen



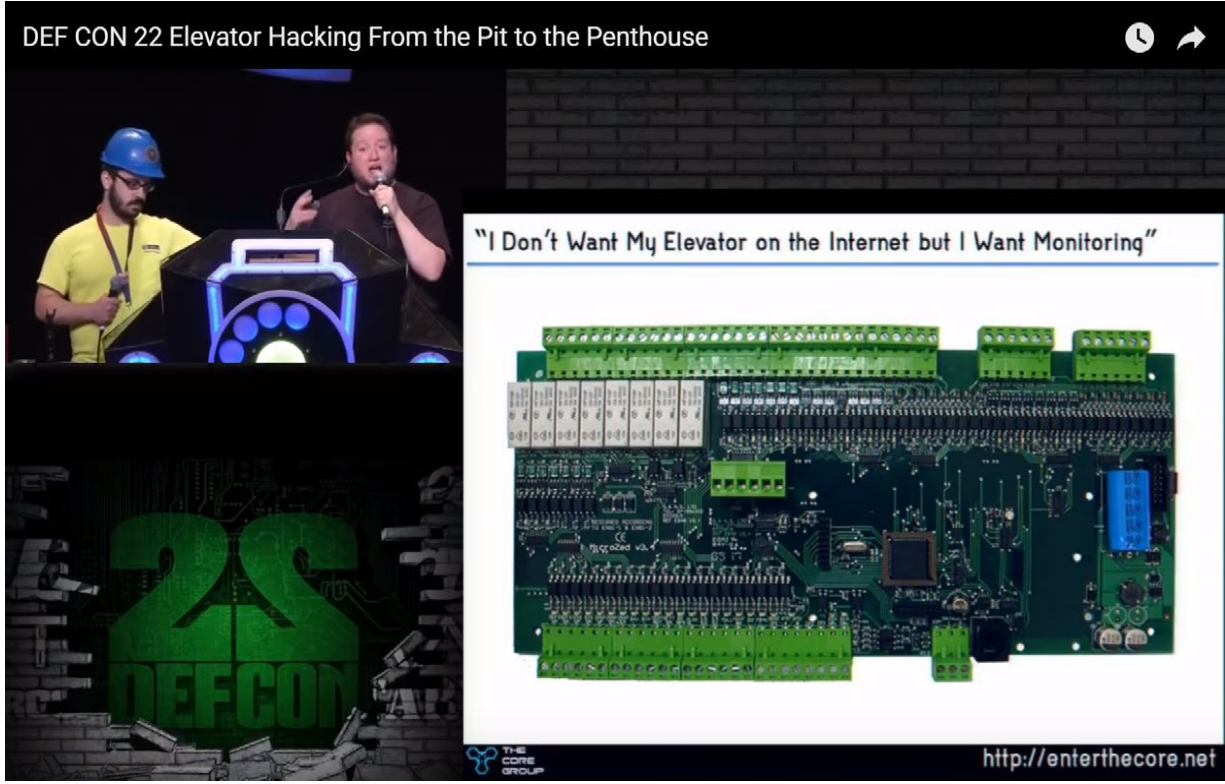
Mythos 3: Systemsteuerungen sind hinter Firewalls sicher!

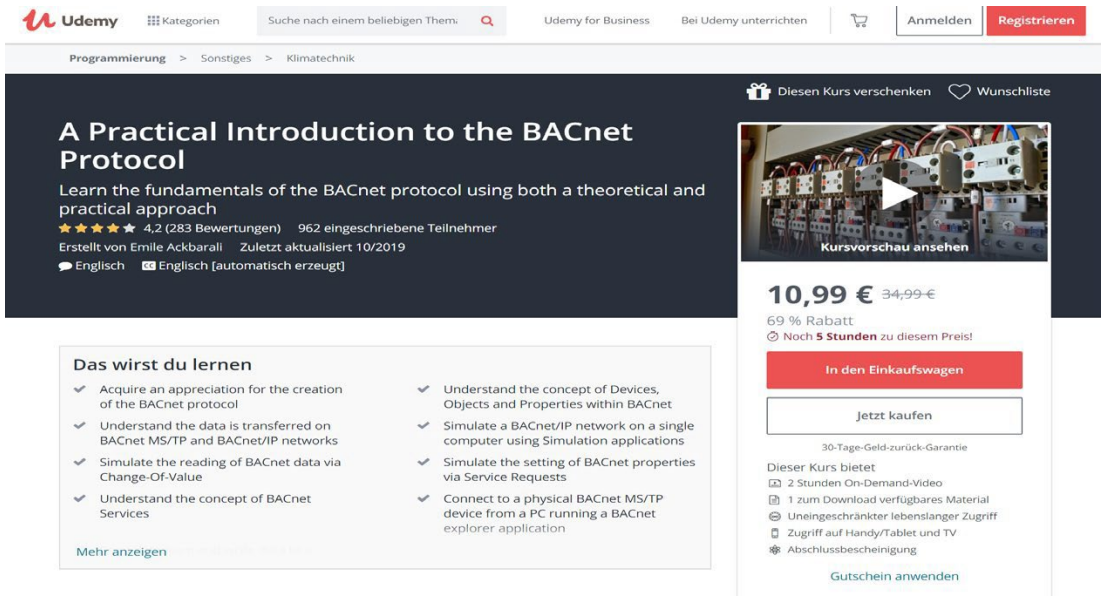
- Firewalls sind nur so sicher wie ihre Konfiguration. Studien an kritischen Infrastrukturen in den USA zeigen, dass über 80 % der Firewalls fehlerhaft konfiguriert sind und somit Schlupflöcher für Angriffe bieten.

- Die Integration von Leit- und Sicherungstechnik über offene Protokolle ist heute üblich.

Mythos 4: Hacker kennen sich nicht mit Automatisierungs-, Kontroll- und Steuerungssystemen aus!

- Hacking ist längst ein Geschäft! Mit Cyberkriminalität wird mittlerweile mehr „Umsatz“ gemacht als mit Drogenhandel.
- SCADA & PLT‘s sind Dauerthemen auf „DEFCON“ und „Blackhat“ Konferenzen.
- Die Informationsangebote der Sicherheitsdienste sind ein zweischneidiges Schwert. Durch zeitnahe Informationen über Sicherheitslücken und Exploits werden Schwachstellen bekannt.
- Online-Kurse vermitteln Wissen über gängige SPS-Systeme oder Gebäudeautomationssysteme.

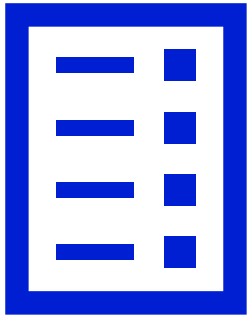




Quellen: Udemy.com & Defcon.org

Gefahrenanalyse an Aufzügen

Wir unterstützen Sie!



Allgemeine Hinweise zur Erstellung einer GBU

+

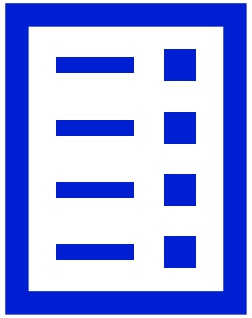
Beschreibung der Aufzugsanlage

+

Gefahrenanalyse

Gefahrenanalyse an Aufzügen

Wir unterstützen Sie!



Allgemeine Hinweise zur Erstellung einer GBU

Dieses Dokument bietet eine Anleitung zur Erstellung einer Gefährdungsbeurteilung für Aufzugsanlagen (Personen- und Lastenaufzüge).

Es klärt über gesetzliche Vorschriften auf, betont die Pflichten des Betreibers und weist Sie bei den jeweiligen Schritten darauf hin, wie der TÜV NORD Sie dabei unterstützen kann.

Abschließend wird der Prozess der Erstellung der Gefährdungsbeurteilung beschrieben, um den gesetzlichen Pflichten gerecht zu werden.

Gefahrenanalyse an Aufzügen

Wir unterstützen Sie!

Beschreibung der Aufzugsanlage

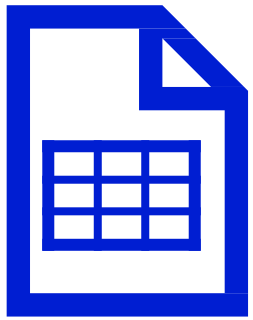
Basierend auf den zentralen Anforderungen der TRBS 1111 bietet dieses Dokument eine detaillierte Übersicht über die Aufzugsanlage.

Diese Erfassung erleichtert die Kommunikation mit Herstellern und Dienstleistern, um spezifische Gefährdungen zu identifizieren und entsprechende Schutzmaßnahmen abzuleiten.

So wird sichergestellt, dass die Anlage dem Stand der Technik entspricht. Durch die sorgfältige Dokumentation der technischen Daten garantieren wir nicht nur die Einhaltung der Richtlinien, sondern auch einen sicheren und effizienten Betrieb des Aufzugs.

Gefahrenanalyse an Aufzügen

Wir unterstützen Sie!



Gefahrenanalyse

Der Kern unserer Dienstleistung ist die Auflistung der Gefährdungen an Ihren Personen- und Lastenaufzügen, die von unseren Sachverständigen identifiziert werden.

Am Ende erhalten Sie zwei Listen:

- **1. Auflistung der Gefährdungen**, die am Aufzug dem aktuellen Stand der Technik entsprechen.
- **2. Auflistung Klärungspunkte:** Sollten aufgrund fehlender Informationen bei der Durchführung der Gefahrenanalyse bestimmte Gefährdungsquellen nicht bewertet werden können, wird der Sachverständige dies ebenfalls vermerken und die betreffenden Punkte in einer Auflistung zusammenfassen.

Gefahrenanalyse an Aufzügen

Wir unterstützen Sie!

Gefahrenanalyse der Aufzugsanlage

Fabriknr. 12345
Betreiber Max Mustermann
Musterstraße 99
45300 Musterstadt

Datum: 07.03.2024
Betriebsort: Max Mustermann
Musterstraße 99
45300 Musterstadt

Zusammenfassung der Gefährdungen

Gefähr-dungen-Nr.	Beschreibung der Gefährdungen	Mögliche Maßnahmen zur Minderung der Gefährdungen (TRBS 3121 bzw. EN81-80)	Datum der Umsetzung	Umgesetzte technische Maßnahme oder Ersatzmaßnahme
5.	Gefährdung aufgrund einer durchbrochenen Schachtumwehrung nahe der Türverriegelungen. (z.B. Reichen durch einen Gitterschacht zur Türverriegelung durch Unbefugte)	Einbau einer vollwandigen Schachtumwehrung gemäß DIN EN 81-20 oder Einbau einer durchbrochenen Schachtumwehrung gemäß DIN EN 81-20		
8.	Gefährdung der betretbaren Räume unterhalb des Schachts mangels fehlender Sicherheitseinrichtung	Einbau einer Fangvorrichtung für das Gegen- oder Ausgleichgewichts nach DIN EN 81-20		
9.	Gefährdung durch fehlende oder unzulängliche Abtrennung der Fahrbahn des Gegengewichts / Ausgleichgewichts	Technische Maßnahme: - Einbau einer Gegengewichts- / Ausgleichgewichtsabtrennung nach DIN EN 81- 20 (bis in 2 m über Schachtgrubensohle und in Breite des Gegengewichtes bzw. Ausgleichgewichts) Organisatorische Maßnahme:		

TÜVNORD

TÜV NORD Gebäudetechnik

Ihr direkter Kontakt zu uns

Nehmen Sie sich bitte 2 Minuten Zeit für die Beantwortung einer kurzen Umfrage:

Sales Center West
T +49 5251 141 120
vertrieb-immo-west@tuev-nord.de

Sales Center Nord
T +49 40 8557 2050
vertrieb_HH@tuev-nord.de

Sales Center Mitte-Ost
T +49 201 825 2412
vertrieb_mitte-ost@tuev-nord.de

gebaeudetechnik@tuev-nord.de

Kommende Gebäudetechnik Webinare

TÜV NORD Gebäudetechnik Webinare

Prüfungen von elektrischen Anlagen leicht gemacht mit TÜV NORD!

- 21.05.2026, 14:00 - 15:00 Uhr

Neue Trinkwasserverordnung und Hygieneerstinspektion an Trinkwasserinstallationen

- 15.10.2026, 14:00 - 14:45 Uhr

Prüfung von Lüftungsanlagen und Hygieneinspektionen nach VDI 6022

- 12.11.2026, 14:00 - 15:00 Uhr

Anmeldungen

- weitere Themen und mehr Informationen finden Sie hier: www.tuev-nord.de/gtd

Sie erreichen uns unter: gebaeudetechnik@tuev-nord.de

Treffen Sie uns auch auf Messen!

TÜV NORD Akademie

Wissen gibt Sicherheit

Seminarempfehlungen Ihres Weiterbildungsspezialisten

Seminar-Nr.:
10201271
Informationsmanagement

OT-Security Manager (TÜV®) nach IEC 62443

OT-Cybersicherheit für Industrial Automation und Control Systems (IACS) nach IEC 62443 und NIS-2

Seminar-Nr.:
10201401
Informationsmanagement

Netzwerksicherheit und Firewall Schulung für IT-Sicherheits- / Informationssicherheitsbeauftragte

ISO 27001, ISO 27033, ISO 27035,
BSI IT-Grundschutz – Grundlagen, Techniken und Anforderungen

Seminar-Nr.:
50201201
Arbeitssicherheit

Schulung: Betriebssicherheitsverordnung (BetrSichV)

Grundlage für Arbeitsschutz und den Schutz Dritter bei überwachungsbedürftigen Anlagen

Präsenz/Online

Im Online-Shop **tuev-nord.de/seminare**
Seminar-Nr. in die Suchmaske eingeben **– Suche starten und alle Seminarinfos finden**

TÜVNORD